



**Lourdes Centeno**  
Socia responsable de Derecho Societario,  
Gobierno Corporativo y Mercados de Capitales

**Raúl García Gonzalez**  
Socio responsable del Área Laboral

**Blanca Escribano Cañas**  
Socia del Área Digital Law

**Iñigo Sebastian de Erice**  
Socio Forensic & Integrity Services

El pasado 21 de febrero, el Congreso de Diputados aprobó el texto final de la Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción (**la “Ley”**), que traspone al ordenamiento jurídico español la Directiva (UE) 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 (la denominada Directiva de *Whistleblowing*).

Tal y como se desprende de su contenido, esta norma tiene como finalidad, por un lado, 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 en su artículo 2 y, por otro, fortalecer y fomentar la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público.

De este modo, la Ley aplicará, entre otros sujetos, a las personas físicas o jurídicas que tengan contratados **cincuenta o más trabajadores**, a partidos políticos y entidades que integran el sector público; y protegerá a las personas que informen a través de cualquier tipo de canal.

El sistema interno de información será el cauce preferente para informar sobre las acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea o infracciones penales o administrativas graves o muy graves, y tendrá como finalidad que la propia organización tenga conocimiento de los posibles daños que reporten tanto empleados como autónomos y terceros ajenos a la organización.

Estas personas quedarán protegidas por un régimen específico que conlleva medidas de protección para el informante, entre las que se encuentra la prohibición expresa de actos constitutivos de represalias (ver sección “¿Qué tienen que tener en cuenta las entidades en materia laboral?”).

La Ley prevé, en el caso de grupo de empresas, que el Sistema interno de información pueda ser único para todo el grupo. Las organizaciones disponen de un plazo máximo de 3 meses para su implementación, con la excepción de las empresas privadas con menos de 250 trabajadores, que dispondrán para ello hasta el 1 de diciembre de 2023.

Se prevé que la aplicación práctica de la Ley tenga un importante impacto en las entidades sujetas a la misma, como mínimo en tres distintos ámbitos: el del cumplimiento normativo, el de la de protección de datos y ámbito laboral.

## ¿Qué impactos son previsibles en el ámbito del Cumplimiento Normativo?

---

La inclusión de mecanismos internos de información de naturaleza análoga a los previstos en esta norma surge en España, esencialmente, a raíz de la inclusión del régimen de responsabilidad de las personas jurídicas, siendo uno de los elementos elementales de los programas de cumplimiento.

De este modo el primer impacto que conlleva afectará, en una primera instancia, a aquellas entidades sujetas por la Ley de acuerdo con los artículos 10 y 13 y que no cuenten con ningún sistema interno de información, pudiéndose concentrar principalmente en el sector privado en organizaciones de dimensión reducida y con carácter general en el ámbito de la Administración Pública.

En una segunda instancia, afectará a aquellas otras entidades que, de una manera u otra, cuenten con mecanismos de similar naturaleza para poder comunicar infracciones o cualquier tipo de irregularidad, generalmente conocidos como canales de denuncia.

En este sentido, una de las grandes novedades que incorpora la Ley aprobada, se refiere a la inclusión de un nuevo tipo de infracción, en su artículo 63, calificada como “*muy grave*” y referida al “*incumplimiento de la obligación de disponer de un Sistema interno de información en los términos exigidos en esta ley*”.

Es importante destacar que, de acuerdo con el artículo 65, este tipo de infracciones “*muy graves*” pueden ser sancionadas pecuniariamente hasta un millón de euros, pero también puede decretarse “*la prohibición de obtener subvenciones u otros beneficios fiscales*” o “*de contratar con el sector público*” durante un plazo máximo de cuatro y tres años, respectivamente.

De este modo, y motivado por el importante impacto que estas sanciones pudieran derivar en el ámbito empresarial privado o público, se considera fundamental la revisión de los sistemas de información vigentes prestando especial atención a los siguientes aspectos que se incluyen como requerimientos de los sistemas internos de información:

### **Aspectos relativos a las responsabilidades organizativas**

El órgano de administración u órgano de gobierno de cada entidad u organismo obligado por la nueva Ley será el responsable de la implantación del sistema interno de información, previa consulta con la representación legal de los trabajadores.

El órgano de administración u órgano de gobierno de cada entidad u organismo deberá designar, destituir o cesar a la persona física responsable de la gestión del sistema interno de información (el “**Responsable del Sistema**”) o, en caso de optarse por un modelo de órgano colegiado para dicha gestión, a las personas físicas integrantes del mismo, una de las cuales será en quien se deleguen las facultades de gestión del sistema interno de información y de tramitación de expedientes de investigación.

El Responsable del Sistema deberá desarrollar sus funciones de forma independiente y autónoma y deberá disponer de todos los medios personales y materiales para ejercer su función adecuadamente. En el caso del sector privado, el Responsable del Sistema será, en principio, un directivo de la entidad. Cuando la naturaleza o dimensión de la entidad no permitan o justifiquen la existencia de un directivo Responsable del Sistema, será posible el desempeño de las funciones propias del puesto o cargo con las de Responsable del Sistema, tratando de evitar posibles situaciones de conflicto de interés.

En los casos de entidades en las que exista una persona responsable de la función de cumplimiento normativo o de políticas de integridad, podrá ser esta la persona designada como Responsable del Sistema, siempre que cumpla los requisitos de la Ley. La designación o cese del Responsable del Sistema deberá comunicarse a la Autoridad Independiente de Protección del Informante (“AIPI”).

### **Aspectos relativos a los requerimientos técnicos de los sistemas internos de información**

Las organizaciones deberán evaluar el cumplimiento de los requerimientos exigidos por la nueva Ley, poniendo especial énfasis en los siguientes aspectos: la apertura del sistema a los informantes comprendidos en el artículo 3 de la Ley; permitir la realización de comunicaciones anónimas, así como verbales o por escrito – o de ambos modos; dotar al sistema de las medidas de seguridad previstas de forma que se garantice la confidencialidad o la adaptación de los canales de denuncia actuales para incluir aquellas novedades que trae la nueva regulación o los plazos previstos de acuse de recibo o resolución de las actuaciones de investigación.

### **Aspectos procedimentales**

La Ley prevé que las entidades cuenten con una política o estrategia que enuncie los principios generales en materia de Sistema Interno de Información y defensa del informante y que sea debidamente publicitada en el seno de la entidad u organismo.

Asimismo, establece la necesidad de aprobar un procedimiento de gestión de informaciones por parte del órgano de administración u órgano de gobierno de cada entidad obligada, siendo el Responsable del Sistema responsable de su tramitación, y que estará dirigido a establecer las previsiones necesarias para que el Sistema interno de

Información cumpla con los requisitos establecidos en la Ley. Cabe destacar entre estos requisitos “*la remisión de la información al Ministerio Fiscal con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito y en el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea*”.

### **Aspectos relativos a la transparencia e información**

En cuanto la publicidad, transparencia y registros de los sistemas de información, le Ley estipula que se deberá proporcionar “*la información adecuada de forma clara y fácilmente accesible, sobre el uso de todo canal interno de información que hayan implantado, así como sobre 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.*”

Además, todos los sujetos obligados “*deberán contar con un libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar*”.

## **¿Qué tienen que tener en cuenta las entidades en materia de protección de datos personales?**

---

El texto legislativo prevé un régimen en línea con lo regulado en el Reglamento General de Protección de Datos (“**RGPD**”) y en la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (“**LOPDGDD**”). No obstante, presenta aspectos específicos que merece la pena tener en cuenta. Mencionamos a continuación algunos de los más relevantes.

### **¿Cuáles son los roles y responsabilidades de los agentes involucrados?**

El órgano de administración u órgano de gobierno de cada entidad u organismo obligado por la nueva Ley adquiere la condición de responsable del tratamiento de los datos personales. Si el sistema se implanta en un grupo de empresas, la Ley sugiere la posibilidad de que suscriban acuerdos para regular la corresponsabilidad en el tratamiento de datos derivados del sistema interno de información, que abarcará al órgano de administración y las diferentes entidades que utilicen el sistema de información. Si la gestión del sistema interno de información se encarga a un tercero externo a la organización, este tercero externo tendrá la consideración de encargado del tratamiento.

### **¿Cuáles son las obligaciones principales en materia de protección de datos?**

La nueva norma impone la obligación de preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y los de cualquier tercero que se mencionen en la información suministrada al sistema de información. Para ello, las empresas deben tomar medidas técnicas y organizativas sobre las revelaciones.

La identidad del informante solo podrá ser comunicada a la autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de la correspondiente investigación, ya sea de carácter penal, disciplinaria o sancionadora.

En cuanto a los deberes de información y transparencia hacia las personas físicas (cuestión no resuelta por completo en la LOPDGDD), la nueva Ley prevé que se informe al denunciante de las condiciones del tratamiento de datos y se incluya de forma expresa que su identidad es reservada y no se comunicará ni a las personas afectadas por los

hechos relatados, ni a terceros. Se exceptúa al deber de información con respecto a la persona afectada por el hecho relatado (puesto que podría frustrar el buen fin de la investigación) y se le priva del derecho de oposición a este tratamiento (salvo que pruebe que no existe un motivo imperioso para continuar con el tratamiento de sus datos).

Por último, se prohíbe la recopilación de datos personales no manifiestamente pertinentes para un expediente concreto y se impone la obligación de destruirlos sin dilación en caso de captarlos por accidente.

### ¿Cuáles son las medidas concretas aplicables al tratamiento?

En cuanto al funcionamiento material de los tratamientos de datos desarrollados en el sistema interno de información, deben tenerse en cuenta ciertas reglas de funcionamiento:

- ▶ **Limitación de los permisos de acceso.** Solo podrá ser accesible al responsable del sistema, al responsable de recursos humanos (si procediera la adopción de medidas disciplinarias a un trabajador), al responsable de servicios legales (si procediera la adopción de medidas legales) y al Delegado de Protección de Datos (“DPD”).
- ▶ **Conservación de los datos en el sistema.** La conservación de los datos objeto de tratamiento deberá realizarse únicamente durante el tiempo imprescindible para decidir la procedencia de iniciar una investigación sobre los hechos informados. En el caso de que no se haya iniciado ninguna investigación, se deberá suprimir la información, en todo caso, transcurridos tres meses desde la recepción. Este plazo, no obstante, es máximo, siendo necesario suprimir la información inmediatamente desde que se tenga constancia de una falta de veracidad en el relato o improcedencia para continuar la investigación. No será posible bloquear los datos (tiene que ser supresión definitiva). Por último, en los casos en los que sea necesaria para el procedimiento judicial, sí se permitirá guardar la información estrictamente necesaria por el tiempo oportuno para las actuaciones.
- ▶ **Anonimización de las denuncias.** Será posible el mantenimiento de denuncias anonimadas (es decir, no vinculables a una persona física y sin posibilidad de inferir identidades) durante plazos indefinidos a los solos efectos de poder demostrar el funcionamiento del propio sistema.
- ▶ **Medidas técnicas de confidencialidad.** El informante tiene derecho a que su identidad sea preservada a terceras personas y el sistema deberá ser diseñado de tal forma desde el momento de la captación de datos.
- ▶ **Comunicación de datos personales.** La identidad del informante sí que puede ser revelada a los organismos jurisdiccionales, Ministerio Fiscal o a la correspondiente autoridad administrativa relevante para la infracción denunciada. Será necesaria la previa información al denunciante acerca de la revelación y sus motivos (salvo peligro de comprometer la investigación).

El DPD será una pieza clave en la salvaguarda de los derechos de los informantes y servirá para generar confianza a la persona que toma la decisión de denunciar una infracción. Puede servir, además, como reflejo de proactividad y atenuante en la aplicación del régimen sancionador. En este sentido, el artículo 76.2 g) LOPDGDD tiene en cuenta, al cuantificar las sanciones y medidas correctivas, la circunstancia de disponer de un DPD cuando no es obligatorio.

## ¿Qué tienen que tener en cuenta las entidades en materia laboral?

---

El Título VII contempla distintas medidas de apoyo a aquellas personas que comuniquen o revelen infracciones previstas en la Ley de protección del denunciante.

### ¿Qué condiciones de protección se prevén?

Se prevé la protección al denunciante siempre y cuando existan motivos para considerar que la información es veraz cuando se comunique y se efectúe conforme a los requerimientos previstos.

Tendrán derecho a protección los informantes que hayan comunicado información de forma anónima, y que posteriormente hayan sido identificados; así como los informantes que informen ante instituciones, órganos u organismos pertinentes de la Unión Europea infracciones incluidas dentro del ámbito de la Directiva (UE) 2019/1937.

Quedan excluidos de la protección las personas que comuniquen informaciones: (i) previstas en comunicaciones inadmitidas por canales internos; (ii) vinculadas a reclamaciones sobre conflictos interpersonales; (iii) que estén públicamente disponibles o sean rumores; y, (iv) que se refieran a acciones u omisiones no contempladas en el ámbito de aplicación de la norma.

### Prohibición de represalias

Se prohíben expresamente actos que constituyan represalias contra personas que presenten una comunicación conforme a lo previsto en la Ley, entendiendo por represalia actos u omisiones que supongan un trato desfavorable que sitúe a la persona que las sufre en desventaja con respecto a otra en el contexto laboral.

Algunos ejemplos a título enunciativo que se mencionan son: evaluaciones negativas, discriminación o trato desfavorable o injusto.

Se contemplan algunas medidas de protección frente a represalias, tal y como se describe a continuación:

- ▶ Las personas que comuniquen información sobre acciones u omisiones no incurrirán en responsabilidades, siempre que se pueda considerar que era necesario al objeto de revelar alguna acción u omisión. Esta medida no afectará a las responsabilidades de carácter penal.
- ▶ Los informantes no incurrirán en responsabilidad respecto de la obtención de la información comunicada públicamente, siempre que se haya accedido a la misma sin cometer un delito.
- ▶ En los casos, ante un órgano jurisdiccional u otra autoridad, en los que el informante demuestre que ha hecho una revelación pública y que ha sufrido un perjuicio, se presumirá que el mismo se produjo como represalia por informar.
- ▶ En procesos judiciales, no se incurrirá en responsabilidad como consecuencia de comunicaciones o revelaciones públicas protegidas por la mencionada Ley.

### **¿Qué medidas de apoyo se contemplan para los informantes?**

Como medidas de apoyo, se contemplan las siguientes:

- ▶ Información y asesoramiento gratuitos sobre procedimientos y recursos disponibles.
- ▶ Asistencia de autoridades competentes ante cualquier autoridad pertinente implicada en protección ante represalias.
- ▶ Asistencia jurídica en procesos penales y civiles transfronterizos.
- ▶ Apoyo financiero y psicológico, si lo decidiese la Autoridad Independiente de Protección del Informante.

### **¿Qué medidas de protección se contemplan para las personas afectadas?**

La Ley incluye los siguientes derechos para los afectados por la comunicación: (i) la presunción de inocencia; (ii) el derecho de defensa; y, (iii) el derecho al acceso al expediente.

### **Supuestos de exención y atenuación de la sanción**

Se contemplan casos en los que se eximirá del cumplimiento de sanciones administrativas a aquellos que hubieran participado en la comisión de infracciones, siempre que informen de la existencia de dicha infracción y que se acredite lo siguiente:

- ▶ Que se haya cesado en la comisión de la infracción e identificado al resto de personas que hubieran participado en ella.
- ▶ Que se coopere plenamente durante la investigación.
- ▶ Que se facilite información veraz y datos significativos.
- ▶ Que se proceda a reparar el daño causado.

### **¿Cuál es el régimen sancionador?**

La autoridad sancionadora competente en este caso será la AIPI, a menos que la competencia se haya atribuido en la normativa autonómica a los organismos autonómicos competentes, sin perjuicio de las facultades disciplinarias que se reconozcan en el ámbito interno de cada organización.

Una de las infracciones calificadas como muy graves es el incumplimiento de la obligación de disponer de un sistema interno de denuncias. Se estima que dicho incumplimiento lleve aparejada una multa entre 600.001 y 1.000.000 de euros, pudiéndose acordar adicionalmente una amonestación pública, la prohibición de obtener subvenciones u otros beneficios fiscales durante un plazo máximo de 4 años o la prohibición de contratar con el sector público durante un plazo máximo de 3 años.

Para la graduación de la sanción se tendrán en cuenta criterios como la reincidencia, la entidad y persistencia del daño, la intencionalidad y culpabilidad, el ejercicio económico inmediatamente anterior, si se subsanó el incumplimiento o si se reparó el daño y la colaboración que se haya prestado con la AIPI.

¡[Suscríbete](#) a las newsletters de EY para mantenerte actualizado!



---

Para cualquier información adicional, contacte con:

**Ernst & Young Abogados, S.L.P.**

Lourdes Centeno Huerta

[Lourdes.Centeno.Huerta@es.ey.com](mailto:Lourdes.Centeno.Huerta@es.ey.com)

Blanca Escribano Cañas

[Blanca.Escribano.Canas@es.ey.com](mailto:Blanca.Escribano.Canas@es.ey.com)

Raúl Luis García Gonzalez

[RaulLuis.GarciaGonzalez@es.ey.com](mailto:RaulLuis.GarciaGonzalez@es.ey.com)

Iñigo Sebastian de Erice

[Ignacio.sebastiandeerice@es.ey.com](mailto:Ignacio.sebastiandeerice@es.ey.com)



**Acerca de EY**

EY es líder mundial en servicios de auditoría, fiscalidad, asesoramiento en transacciones y consultoría. Los análisis y los servicios de calidad que ofrecemos ayudan a crear confianza en los mercados de capitales y las economías de todo el mundo. Desarrollamos líderes destacados que trabajan en equipo para cumplir los compromisos adquiridos con nuestros grupos de interés. Con ello, desempeñamos un papel esencial en la creación de un mundo laboral mejor para nuestros empleados, nuestros clientes y la sociedad.

EY hace referencia a la organización internacional y podría referirse a una o varias de las empresas de Ernst & Young Global Limited y cada una de ellas es una persona jurídica independiente. Ernst & Young Global Limited es una sociedad británica de responsabilidad limitada por garantía (company limited by guarantee) y no presta servicios a clientes. Para ampliar la información sobre nuestra organización, entre en [ey.com](http://ey.com).

© 2023 Ernst & Young Abogados, S.L.P.

Todos los derechos reservados.

ED None

La información recogida en esta publicación es de carácter resumido y solo debe utilizarse a modo orientativo. En ningún caso sustituye a un análisis en detalle ni puede utilizarse como juicio profesional. Para cualquier asunto específico, se debe contactar con el asesor responsable.

[ey.com/es](http://ey.com/es)

Twitter: [@EY\\_Spain](https://twitter.com/EY_Spain)

LinkedIn: [EY](https://www.linkedin.com/company/ey)

Facebook: [EY Spain Careers](https://www.facebook.com/EY_Spain_Careers)

Google+: [EY España](https://www.google.com/search?q=EY+Espa%C3%B1a)

Flickr: [EY Spain](https://www.flickr.com/photos/ey-spain/)