Whistleblowing. Ley de Protección del Informante

Ya ha entrado en vigor 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 ("**Ley de Protección del Informante**", "**LPI**"), que Transpone la Directiva 2019/1937 ("**Directiva de Whistleblowing**"), complemento necesario de la prevención y detección del incumplimiento y de la corrupción, aplicable a entidades y organizaciones privadas y públicas, prohibiendo represalias contra el Informante y su entorno, con medidas de protección incluso asistenciales y financieras. A continuación abordamos los aspectos clave de la LPI

Comunicaciones que dan derecho a la Protección del Informante: Las referidas a hechos delictivos, a infracciones administrativas graves o muy graves, e infracciones del Derecho UE o intereses UE, excluyendo información clasificada o que afecte a la Seguridad del Estado.

Personas protegidas: Toda persona que en un **contexto laboral o profesional** haya accedido a información sobre presuntas infracciones ("**Informante**") y a su entorno -ej. familiares, compañeros, entidades en que trabaje, o de las que sea titular-. Se admite la denuncia anónima.

Sistemas o canales de información: A). Canal Interno: En general, toda entidad de 50 o más trabajadores, y Grupos de Empresas deben disponer de un único **sistema interno de información** ("**SII**") que integre todos sus canales de denuncia (ej., de prevención del acoso, de la prevención de delitos o infracciones del código ético o del programa de prevención) y que cumpla una serie de requisitos – ej. protocolos, garantías, confidencialidad de informante y de la(s) persona(s) afectadas, datos personales) y **designar a un directivo como responsable** (puede asumir esta función el órgano responsable de cumplimiento) que se notificará a la A.A.I. El plazo de implantación es de 3 meses, si bien para entidades de menos de 250 trabajadores se amplía al 01 de diciembre de 2023. **B). Canales Externos: Autoridad Independiente de Protección al Informante ("A.A.I."-**Autoridad Administrativa Independiente), -estatal- encargada de gestionar el Canal Externo con potestades sancionadora, y de apoyo a los informantes. Toda persona física podrá informar ante la AAI (o a los órganos autonómicos) directamente o previa comunicación por el canal interno. Se permite la vía de **Revelación Pública** de información en ciertos casos -ej. haber intentado los canales internos y externos o en peligro inminente – no exigibles en comunicación a la prensa, en el ejercicio de la libertad de expresión y de información veraz.

Sistema de Información Interno ("**SII**")

El sistema de información interno del sector privado (empresarios, sociedades asociaciones, fundaciones, etc.) debe cumplir con los siguientes **principios y requerimientos esenciales:**

a) Accesible a todas las personas sujeto de protección según la Ley.

b) Deben permitirse **denuncias anónimas**.

c) Garantía de confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación (ej persona(s) "denunciada(s)" y del tratamiento de la información y su investigación.

d) Garantías frente a la adopción de represalias.

e) Presunción de inocencia

f) Derecho de defensa de las partes afectadas.

g) Independencia, imparcialidad

h) Ausencia de conflictos de interés.

i) Tramitación efectiva de las comunicaciones y su archivo: el sistema debe guardar trazabilidad y recuperación de las actuaciones de la tramitación.

j) Cumplimiento de la normativa sobre protección de datos personales.

Política de In+Formación que enuncie los principios generales del sistema en la organización y el funcionamiento del SII, en especial, información se los canales que integran el SII a disposición de los posibles informantes, así como información clara y accesible sobre información de los canales externos de información – A.A.I. y ante las instituciones de la UE.

Página web: debe incluir, en su página de inicio (en sección fácilmente identificable) información clara y accesible sobre el uso de todo SII de información implantado, y los principios del procedimiento de gestión.

Procedimiento de gestión de comunicaciones, aprobado por el órgano de administración con los siguientes elementos mínimos:

1º) Presentación de las comunicaciones, deben permitirse en forma

Verbal: por vía telefónica o por sistema de mensaje de voz. Además, previo consentimiento del informante, o, si lo solicita el informante agendar una reunión presencial para su celebración en 7 días desde que se reciba la solicitud y deberán documentarse mediante una grabación o transcripción, ofreciendo al informante la posibilidad de revisarla y firmarla en este último supuesto;

y

Escrita: por correo postal o por cualquier medio electrónico habilitado al efecto.

El Informante podrá indicar el medio en el que prefiere recibir las notificaciones sobre el tratamiento de la comunicación, indicando domicilio, correo electrónico o lugar seguro a tal efecto. Se permite mantener una vía de comunicación con el informante y de solicitarle información adicional.

Cuando se reciba una comunicación debe procederse en todo caso, con el siguiente protocolo:

2º) **Acusar recibo** al informante en el plazo máximo de **7** días.

3º) **Informar a la persona denunciada** y de los derechos que le asisten tales como: a que se le informe de las infracciones que se le atribuyen, a ser oída en cualquier momento, al honor, a la defensa, presunción de inocencia.

4º) El SII debe tener establecido un **plazo máximo para responder a las comunicaciones recibidas** de 3 meses a partir del vencimiento del plazo de 7 días después de la comunicación, salvo casos de especial complejidad, ampliable por otros **3** meses.

5º) **Confidencialidad** respecto de todas las comunicaciones que se cursen a través del SII o de otros canales o personas distintas de las previstas en el sistema, debiendo formarse expresamente al personal en esta materia.

6º) **Protección de datos personales**: debe cumplirse con la normativa en cuanto a la conservación y eliminación de **datos personales**. En particular, comunicaciones podrán mantenerse en el SII 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 3 meses, deberá suprimirse del sistema la comunicación, salvo con el fin de mantener evidencia del funcionamiento del sistema y de forma anonimizada. Es conveniente asegurarse que los sistemas deben permitan cumplir con estas obligaciones de supresión.

7º) **Denuncia a Fiscalía**: Obligación de remitir la información al **Ministerio Fiscal** cuando los hechos pudieran ser indiciariamente constitutivos de delito **y a la Fiscalía Europea** cuando afecten a los intereses financieros de la UE – y ello, sin perjuicio, en su caso, de los derechos de la organización a no confesarse culpable y a defenderse.

8º) **Libro-registro de comunicaciones** recibidas e investigaciones realizadas: Debe mantenerse al día en la entidad, al que sólo pueden acceder los jueces en el marco de un procedimiento judicial.

Externalización de tareas: Se prevé la **posibilidad de externalizar la gestión del SII** a través de tercero si bien la gestión por tercero externo no implica traslado de las obligaciones de la entidad responsable del SII.

Sanciones: El incumplimiento o implementación defectuosa de SII, supone sanciones que podrán ser publicadas en el BOE y que pueden alcanzar 1.000.000 € además de amonestación pública, prohibición de acceder a subvenciones o beneficios fiscales durante 4 años y de contratar con el sector público durante 3 años – sin perjuicio de las sanciones en protección de datos personales.

Comentario general: Con este nuevo conjunto de obligaciones, dado que cualquier denunciante podrá elegir entre los canales externos o internos, se hace imprescindible ya adoptar las medidas para cumplir y a la vez gestionar la información. En todo caso, recordar que, según el art. 31 bis 5.4º del Código Penal, cualquier empresa u organizaciones en general tiene ya obligación de establecer canales para informar de posibles riesgos e incumplimientos al responsable de cumplimiento como condición para evitar la responsabilidad penal de la entidad.

Maria Antonia Garcia-Solanas