

Sistema interno de información



White paper

NOVEDADES

Novedades normativas tras la publicación de la Ley 2/2023, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

**marzo
2023**

CONTENIDO

01 ANTECEDENTES

Marco normativo para los canales de comunicación

02 FINALIDAD Y ÁMBITO DE APLICACIÓN

Finalidad del Sistema interno de información. Ámbito objetivo y subjetivo

03 ¿QUIÉN O QUIENES ESTÁN OBLIGADOS A IMPLANTAR Y GESTIONAR UN SII?

Sujetos obligados y plazos de implantación

04 SISTEMA INTERNO DE INFORMACIÓN (SII)

Pasos a seguir para implantar un SII.
La protección de datos en el SII
Proceso de gestión.

El Sistema interno de información para empresas y organismos públicos se concibe como la vía de comunicación, interna y externa, a través de la cual se reciben y gestionan las denuncias (o comunicaciones) realizadas por los miembros de la organización o por otras personas vinculadas a ella, sobre posibles comportamientos irregulares o ilícitos de las que tengan conocimiento o hayan sido testigos.

01. Antecedentes: Marco normativo para los Canales de comunicación



En el marco normativo sobre el que se basa el nuevo Sistema de Información Interna; se pueden citar, por un lado, la **Ley Orgánica 5/2010 y 1/2015** de modificación del Código Penal, donde se recoge el plan de prevención de riesgos penales, que debe contar con la implantación de un canal de denuncias. Y por otro lado, está la **Directiva UE 2019/1937**, más conocida como **Directiva Whistleblowing**.

Dada la publicación de la nueva **Ley 2/2023**, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, entrada en vigor en 13 de marzo, donde se incorpora al Derecho español la **Directiva (UE) 2019/1937**, aparece un «nuevo significado» para el Canal de denuncias de las organizaciones, que **está relacionado con el compliance** y con la citada **Ley de protección de los denunciantes**. En este contexto, el Canal de denuncias es el nuevo **Sistema de información Interna** (en adelante, SII).

Este cambio de nombre, incorporándose al Derecho español la Directiva (UE) 2019/1937, se debe principalmente a que en ella se habla de «informantes» y no «denunciantes» y de «comunicaciones» en vez de «denuncias» (ya que la denuncia como concepto jurídico en nuestro Derecho tiene ciertas consideraciones que aquí no aplican o aplican de forma diferente, como por ejemplo, el hecho de que la denuncia pueda ser anónima).

La **Ley 3/2018**, de Protección de datos personales y garantía de derechos digitales, contempla la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad, incluso anónimamente, la comisión, en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que fuera aplicable.

Actualmente, **las organizaciones con un plan de compliance**, sea este por obligación o voluntario (por ejemplo, la adopción de un plan de compliance penal para garantizar el cumplimiento de la normativa en relación a la responsabilidad penal de las organizaciones), **tendrán ya implementado un canal ético o canal de denuncias** (por ejemplo, en empresas obligadas en materia de prevención del blanqueo de capitales). Estas organizaciones **solo deberán preocuparse de que su sistema interno de información se ajuste a la presente normativa**.

Las organizaciones obligadas por la Ley 2/2023, tienen por delante unos meses para adoptar **nuevos sistemas de información y coordinar estos canales con otros protocolos, códigos y políticas internas que puedan tener**.

No existe un único canal de información, sino que las comunicaciones o informaciones de las infracciones o irregularidades se podrán canalizar a través de:

- El canal interno de la empresa.
- El canal externo o Autoridad Independiente de Protección al Informante (AAI).



02. Finalidad y ámbito de aplicación.

La **finalidad** de la norma es la de **proteger a las personas** que en un contexto laboral o profesional **detecten infracciones penales o administrativas graves o muy graves** y las comuniquen mediante los mecanismos regulados en la misma. Además, resulta importante asentar en la sociedad la conciencia de que **debe perseguirse a quienes quebrantan la Ley y que no deben consentirse ni silenciarse los incumplimientos**.

El canal o cauce que facilite estas comunicaciones será a través del establecimiento de **canales internos y externos** en las organizaciones.

Los **canales internos** harán que las informaciones sobre las prácticas irregulares se conozcan por la propia organización para corregirlas o repararlas lo antes posible. Y además, de éstos canales internos, se exigirá la determinación de otros **canales** de información, denominados **<<externos>>**, con el fin de ofrecer a los ciudadanos una comunicación con una autoridad pública especializada, lo que les puede generar más confianza al disipar el temor a sufrir alguna represalia en su entorno. Se considera beneficioso que la habilitación de dicho canal, como medio complementario al canal interno, se encauce a través de la **Autoridad Independiente de Protección del Informante (AAI)**, dotándolo, así, de las garantías de independencia y autonomía exigidas por la norma europea.

Se ha de destacar que se permitirá la **comunicación anónima**, es decir, posibilidad de presentación y tramitación de comunicaciones anónimas. Ahora bien, esto se exceptúa cuando, bien una norma nacional prevé revelarlo, o bien se solicita en el marco de un proceso judicial, argumentando el juzgador la necesidad de conocer la identidad de quien denunció, para garantizar el derecho de defensa del denunciado.



"Resulta importante asentar en la sociedad la conciencia de que debe perseguirse a quienes quebrantan la Ley y que no deben consentirse ni silenciarse los incumplimientos".



Ámbito objetivo

Además de **proteger a quienes informen sobre las infracciones** del Derecho de la Unión previstas en la Directiva del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, esta Ley también abarca las **infracciones penales y administrativas graves y muy graves** de nuestro ordenamiento jurídico.

Ámbito subjetivo

Se extiende la protección a todas aquellas **personas que tienen vínculos profesionales o laborales con entidades tanto del sector público como del sector privado**, aquellas que ya han finalizado su relación profesional, voluntarios, trabajadores en prácticas o en periodo de formación, así como, personas que participan en procesos de selección. **También se extiende la Ley a personas que prestan asistencia a los informantes.**

03. ¿Quienes o quién está obligado a implantar un SII?

Sector privado

Las empresas de **más de 50 personas trabajadoras** tendrán que implantar un sistema interno de información.

El órgano de administración de la empresa es el **responsable de la implantación del sistema**, previa consulta con la representación legal de las personas trabajadoras.

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.

El **plazo para ello es de 3 meses** desde la fecha de entrada en vigor de la Ley, hasta el 13 de junio de 2023 para las empresas con más de 249 personas trabajadoras en plantilla y hasta el 1 de diciembre de 2023 para las empresas con una plantilla de entre 50 y 249 personas trabajadoras.

Se exige que las entidades admitan y tramiten **denuncias anónimas**, además de las comunicaciones por otras vías que permitan la identificación del informante.

"Se exige la integración de todos los canales de las entidades en un único sistema interno de información, garantizando así que la recepción y tramitación de todas las comunicaciones sobre potenciales infracciones cumplan las exigencias de la Ley 2/2023."

Sector 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.

En los **grupos de empresas**, la sociedad dominante (i) aprobará una política general relativa al SII y a la defensa del informante y (ii) 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 de menor tamaño** (entre 50 y 249 trabajadores) podrán compartir entre sí el SII y los recursos destinados a la tramitación de las comunicaciones, respetando en todo caso las garantías previstas en la ley.

Los municipios de menos de 10.000 habitantes, entre sí o cualesquiera otras Administraciones públicas que se ubiquen dentro del territorio de la Comunidad Autónoma, podrán compartir el SII y los recursos destinados a las investigaciones y las tramitaciones.

Asimismo, la Ley 2/2023 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.).



04. Sistema Interno de Información

Las entidades que cuenten con una **página web** deberán incluir en su página de inicio (en una sección separada y fácilmente identificable) información clara y accesible sobre el uso de todo canal interno de información que hayan implantado, así como sobre los principios esenciales del procedimiento de gestión. De igual manera, los sujetos obligados deberán disponer de un **libro-registro** de las comunicaciones recibidas y las de investigaciones realizadas. Dicho registro **no será público y únicamente podrán acceder a él los jueces y tribunales** en el marco de un procedimiento judicial.

Los **datos personales** relacionados con las comunicaciones e investigaciones únicamente **se conservarán** durante el período que fuese necesario, que en ningún caso podrá superar los **diez años**.

Los **principios esenciales** del SII 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.**

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.

Pasos para implementar un Sistema Interno de Información



04. Sistema Interno de Información

Estructura básica del Reglamento del Sistema de Información Interna

Para la elaboración del **Reglamento del SII** se podrá tomar como guía la siguiente estructura básica, como **ejemplo**:

CONTENIDO

- *Introducción y marco normativo.*
- *Ámbito de aplicación.*
- *Órgano competente para su recepción tramitación.*
- *Vías de comunicación del canal para remitir denuncias (email, teléfono, dirección postal, web...).*
- *Requisitos de la denuncia.*
- *Plazos de gestión de las comunicaciones.*
- *Derechos de denunciantes y denunciados.*
- *Funcionamiento del proceso de recepción y tratamiento de las comunicaciones.*
- *Funcionamiento del proceso de evaluación e investigación de las comunicaciones.*
- *Revisión y actualización del canal de comunicaciones.*
- *Medidas de mejora.*
- *Conservación de la información.*

La protección de datos en el SII

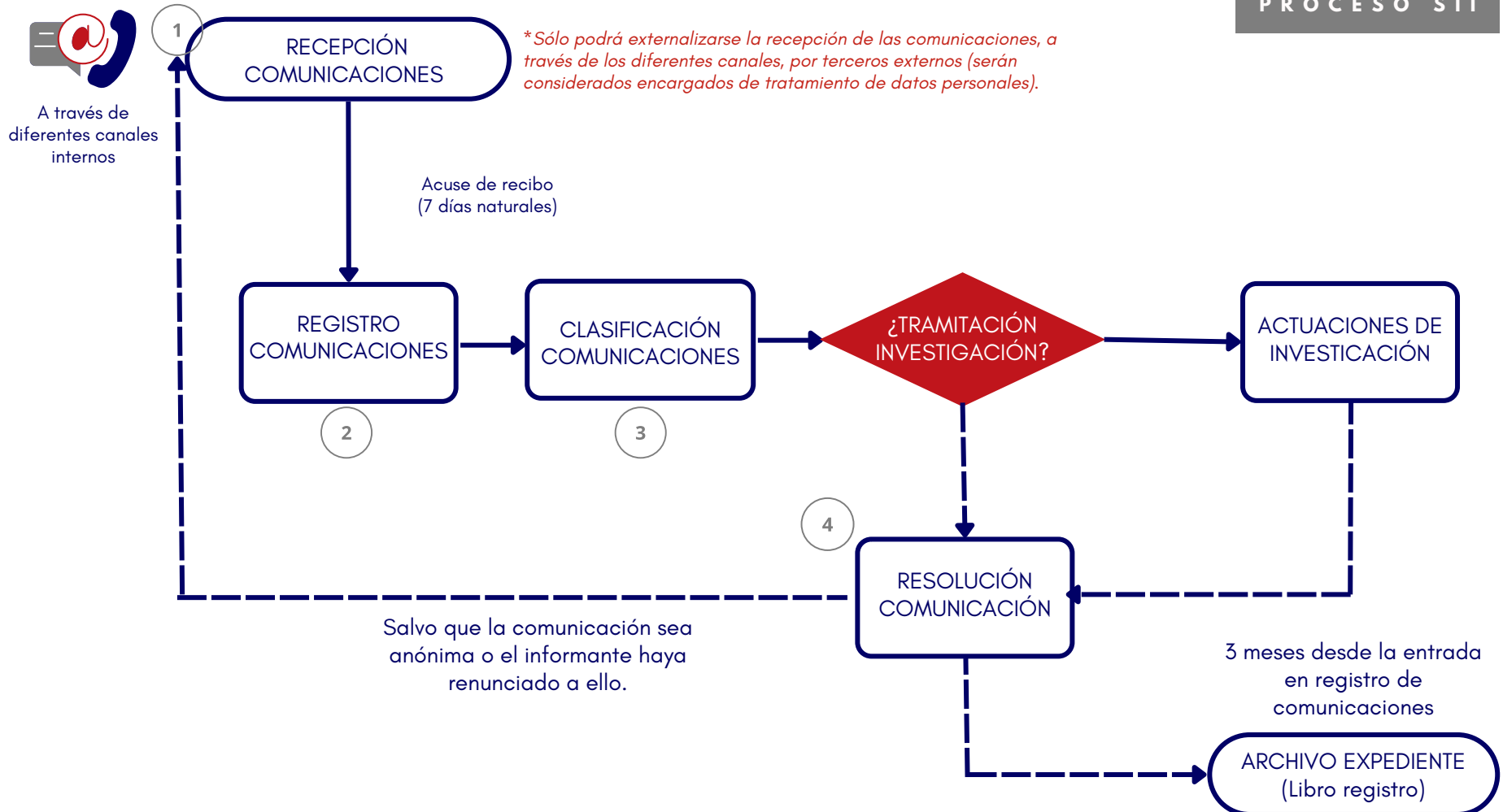
Tan importante como la existencia de protocolos o políticas de gestión en casos de denuncias, la **ley 2/2023** también hace hincapié en una correcta protección de los informantes en sistemas internos, públicos o privados, o en canales externos o revelaciones públicas, se recogen en los arts. 29 y ss. de la Ley:

- **Se registrá conforme a las reglas de RGPD y LOPDGDD** para cada uno de ellos.
- **La información a proporcionar a los interesados y las posibilidades de ejercicio de sus derechos.** La Ley también añade que «no se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una información específica o, si se recopilan por accidente, se eliminarán sin dilación indebida».



- La importancia de la **preservación tanto de la identidad del informante como de las personas investigadas**, que solo puede ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora (art. 33).
- La importancia de contar con un **Delegado de Protección de Datos** competente, que sea competente para toda la gestión en los sistemas internos de comunicaciones (art. 34).

04. Sistema Interno de Información



04. Sistema Interno de información

PROCESO SII



1

CANALES INTERNOS DE COMUNICACIÓN DE INFORMACIONES. El responsable del SII deberá facilitar que se produzcan por diferentes canales:

- Escritas
- Teléfono
- Anónimas
- Reunión presencial a petición del informante.

Independientemente del canal, **la recepción de las comunicaciones deberá diseñarse, establecerse y gestionarse de forma segura:**

- Informar sobre el tratamiento de datos.
- Confidencialidad de la comunicación.
- Posibilitar el anonimato del informante cuando así lo requieran.
- Cumplimiento de plazos.
- Comunicación de Política que enuncie principios generales y defensa del informante.
- Comunicación procedimiento de gestión de informaciones recibidas.
- Comunicación garantías de protección de los informantes.
- ARCHIVO.

2

REGISTRO DE COMUNICACIONES.

Las comunicaciones recibidas, para su mejor gestión, pueden registrarse de forma documental en orden de fecha de registro.

3

CLASIFICACIÓN DE COMUNICACIONES

Las comunicaciones recibidas, una vez registradas en el SII de la organización, deberán clasificarse para determinar si es necesario una evaluación e investigación de la misma o archivarla, ya que, no se considera una información incluida dentro del artículo 2 de la Ley 2/2023.

El archivo de la clasificación de la comunicación podría incluir:

- Código identificación de la denuncia
- Fecha de registro
- Breve descripción de hechos
- Clasificación (prioritaria, no prioritaria, archivo y cierre)

4

RESOLUCIÓN DE COMUNICACIONES

Aquellas comunicaciones que se hayan clasificado para ser evaluadas o investigadas, podrán adjuntar al registro de clasificación:

- Actuaciones realizadas
- Conclusiones
- Resolución



GramAudit



GRAMAUDIT S.L.P.



gramaudit.com

Miembro de la
red

ADN GRM
AUDIT

