Autoridad Independiente
de Protección del Informante

Recomendación

1/2026 de la Autoridad Independiente de Protección del Informante

para el diseño e implementación de un Sistema Interno de Información

Madrid, enero de 2026

Autoridad Independiente de Protección del Informante

Recomendación 1/2026 de la Autoridad Independiente de Protección del Informante para el diseño e implementación de un Sistema Interno de Información.

Índice

INTRODUCCIÓN

La Autoridad Independiente de Protección del Informante, A.A.I. (AIPI) es el organismo público creado por 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, que tiene como fines garantizar la protección de la persona informante, servir de pilar institucional en la prevención y la lucha contra la corrupción, y en la garantía de la integridad de las administraciones y del personal al servicio del sector público, actuando en coordinación en su caso, con otros organismos de control ya existentes en la Administración del Estado y con autoridades similares de otras administraciones territoriales.

Entre sus funciones se encuentran la de gestionar el canal externo de comunicaciones regulado en el título III de la Ley, adoptar las medidas de protección al informante previstas en su ámbito de competencias, informar preceptivamente los anteproyectos y proyectos de disposiciones generales que afecten a su ámbito de competencias y a las funciones que desarrolla, tramitar los procedimientos sancionadores e imponer sanciones por las infracciones previstas en el título IX en su ámbito de competencias y fomentar y promover la cultura de la información.

El artículo 51 de la Ley 2/2023, dispone que *"la persona titular de la presidencia de la AIPI podrá elaborar circulares y recomendaciones que establezcan los criterios y prácticas adecuados para el correcto funcionamiento de la Autoridad".*

Esta Autoridad, desde su puesta en funcionamiento en septiembre de 2025, ha recibido numerosas consultas y ha constatado la existencia de dudas interpretativas sobre cómo poner en marcha diseño e implementación del Sistema Interno de Información (SII) recogido en la Ley 2/2023, de 20 de febrero, y sus elementos relacionados, tales como el canal interno de información y su gestión, tanto en el ámbito público como en el privado. Así, esta Presidencia considera necesario establecer pautas de funcionamiento sobre el cumplimiento de las obligaciones de la Ley respecto a los sistemas internos de información, proporcionando los estándares para que el SII pase de ser una obligación reactiva a una herramienta preventiva proactiva, respetando en cualquier caso las competencias de las administraciones públicas y sin que tenga carácter normativo ni vinculante.

En este sentido, la presente Recomendación 1/2026 adopta un enfoque general, con el objetivo de resolver dudas frecuentes y ofrecer aclaraciones interpretativas transversales. No obstante, se prevé la futura aprobación de recomendaciones específicas para atender a colectivos concretos que, por su singularidad, requieran un tratamiento especial. Todo ello, sin perjuicio de que tanto esta como las futuras recomendaciones puedan ser objeto de revisión, publicándose nuevas versiones o ediciones que las mejoren o actualicen.

En virtud de todo ello, se aprueba la siguiente **RECOMENDACIÓN**.

Recomendación 1/2026 de la Autoridad Independiente de Protección del Informante para el diseño e implementación de un Sistema Interno de Información

I. OBJETIVO Y DESTINATARIOS

La presente Recomendación es un manual de cumplimiento técnico; pero también constituye el instrumento esencial para observar el mandato legal de fomentar la cultura de la información y de la integridad en las organizaciones, que se encuentra entre las funciones de esta Autoridad en virtud del artículo 43.5 de la Ley. El Sistema Interno de Información (SII) es, en esencia, una infraestructura básica sobre la que se asienta una gobernanza ética moderna.

La vinculación entre el diseño del sistema y la integridad institucional emana directamente de la Ley 2/2023, de 20 de febrero. En concreto, el artículo 1 de la Ley establece que la finalidad de la norma no es solo proteger al informante, sino también fortalecer la cultura de la información, de las infraestructuras de integridad de las organizaciones y fomentar la cultura de la información como mecanismo para prevenir y detectar amenazas al interés público, atribuyendo a la AIPI la potestad de fomentar la cultura de la integridad en el sector público y privado, así como velar por la protección del informante.

Por tanto, esta Recomendación materializa el ejercicio de las competencias de la AIPI proporcionando los estándares para que el SII pase de ser una obligación reactiva a una herramienta preventiva proactiva para todas las organizaciones obligadas por la Ley.

La implementación de esta Recomendación permite que el SII funcione como un elemento de aprendizaje organizacional. Al identificar y tramitar las informaciones recibidas:

1. Se detectan infracciones legales antes de que dañen la reputación de la organización y se consoliden como prácticas habituales.
2. Se posibilita la adopción de medidas correctoras eficaces para poner fin a las conductas detectadas, reparar sus efectos y prevenir su reiteración.
3. Se refuerza el mensaje de que todas las personas de la organización son guardianas de la legalidad.
4. Se reduce el espacio para la impunidad, consolidando un entorno de trabajo basado en la responsabilidad compartida.

La adopción de las pautas contenidas en esta Recomendación asegura que el Sistema Interno de Información no sea un mero buzón, sino el corazón de una estrategia integral de cumplimiento, bajo la supervisión y garantía de la AIPI y, en su caso, los órganos autonómicos.

II. ANÁLISIS DEL MARCO NORMATIVO RELATIVO AL SISTEMA INTERNO DE INFORMACIÓN EN LA LEY 2/2023 (LPI)

II.1. Configuración del Sistema Interno de Información (SII)

El Sistema Interno de Información no se limita a un buzón de denuncias; constituye una infraestructura de integridad que debe ser aprobada por el órgano de administración o equivalente de la entidad.

II.1.1. Sujetos obligados (Arts. 10 y 13 LPI)

A) Sector privado (Art. 10)

La obligación afecta a toda persona física o jurídica del sector privado que tenga presencia organizada o establecimiento en España o que desarrolle en el país actividades a través de sucursales o agentes o incluso mediante prestación de servicios sin establecimiento permanente (con independencia del domicilio social) y que se encuentre en alguno de los supuestos previstos en los apartados siguientes.

a) Las personas físicas o jurídicas del sector privado que tengan contratados cincuenta o más trabajadores. La obligación afecta a toda persona física o jurídica del sector privado que tenga presencia organizada o establecimiento en España o que desarrolla en el país actividades a través de sucursales o agentes o incluso mediante prestación de servicios sin establecimiento permanente y que supere el umbral citado de los cincuenta trabajadores en España.

Para determinar si una empresa alcanza el umbral de cincuenta o más trabajadores, puede tomarse como criterio orientativo el establecido en el artículo 3 del Real Decreto 901/2020, de 13 de octubre, por el que se regulan los Planes de Igualdad

A estos efectos:

- Se computa la plantilla total de la empresa, con independencia del número de centros de trabajo, o de la forma de contratación laboral.
- Se incluyen todas las personas trabajadoras, con independencia de la modalidad contractual (contratos indefinidos, fijos discontinuos, contratos de duración determinada, contratos de puesta a disposición (ETT).
- Las personas con contrato a tiempo parcial computan como una persona trabajadora más, con independencia del número de horas.

- Deben añadirse los contratos de duración determinada extinguidos en los seis meses anteriores al momento del cómputo. Cada 100 días trabajados se computa como una persona trabajadora adicional.
- El cómputo debe realizarse, al menos, el último día de los meses de junio y diciembre de cada año, a efectos de verificar si se alcanza el umbral legal.

En todo caso, computan en España a estos efectos, los teletrabajadores que prestan servicios desde el extranjero y los trabajadores desplazados al extranjero

b) Con independencia del número de trabajadores contratados, 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 que se refieren las partes I.B y II del anexo de la Directiva (UE) 2019/1937, del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, deberán disponer de un Sistema interno de información que se regulará por su normativa específica con independencia del número de trabajadores con que cuenten. En estos casos, esta ley se aplicará en lo no regulado por su normativa específica.

En el caso de que la normativa específica contemple la existencia de canales de denuncias, será de aplicación dicha normativa, sin perjuicio de su adaptación a las exigencias de los Sistemas internos de información de la Ley 2/2023.

Se consideran incluidas en el párrafo anterior las personas jurídicas que, pese a no tener su domicilio en territorio nacional, desarrollen en España actividades a través de sucursales o agentes o mediante prestación de servicios sin establecimiento permanente.

c) Con independencia del número de trabajadores contratados, los partidos políticos, los sindicatos, las organizaciones empresariales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos.

B) Sector público (Art. 13)

1. Estarán obligadas las siguientes entidades del Sector Público:

a) La Administración General del Estado, las Administraciones de las comunidades autónomas, ciudades con Estatuto de Autonomía y las entidades que integran la Administración Local.

Concretamente, los municipios de menos de 10.000 habitantes que se ubiquen dentro de una misma Comunidad Autónoma podrán compartir el SSII (Artículo 14 LPI).

b) Los organismos y entidades públicas vinculadas o dependientes de alguna Administración pública, así como aquellas otras asociaciones y corporaciones en las que participen Administraciones y organismos públicos.

c) Las autoridades administrativas independientes, el Banco de España y las entidades gestoras y servicios comunes de la Seguridad Social.

d) Las universidades públicas.

e) Las corporaciones de Derecho público.

f) Las fundaciones del sector público. A efectos de esta ley, se entenderá por fundaciones del sector público aquellas que reúnan alguno de los siguientes requisitos:

1.º Que se constituyan de forma inicial, con una aportación mayoritaria, directa o indirecta, de una o varias entidades integradas en el sector público, o bien reciban dicha aportación con posterioridad a su constitución.

2.º Que el patrimonio de la fundación esté integrado en más de un cincuenta por ciento por bienes o derechos aportados o cedidos por sujetos integrantes del sector público con carácter permanente.

3.º Que la mayoría de derechos de voto en su patronato corresponda a representantes del sector público.

g) Las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de entidades de las mencionadas en las letras a), b), c), d) y g) del presente apartado sea superior al cincuenta por ciento, o en los casos en que, sin superar ese porcentaje, se encuentre respecto de las referidas entidades en el supuesto previsto en el artículo 5 del texto refundido de la Ley del Mercado de Valores.

2. Los órganos constitucionales o sus correlativos a nivel autonómico.

II.1.2. Consulta y aprobación (Art. 5.1 LPI)

La implantación del Sistema requiere la consulta previa a los sindicatos o a la representación legal de las personas trabajadoras de la organización que se trate. La aprobación final corresponde al órgano de gobierno de la entidad, quien es el responsable último de su implantación.

II.1.3. Elementos mínimos, características y principios del SII (Art. 5.2 LPI)

El Sistema Interno de Información, en cualquiera de sus fórmulas de gestión (propia o compartida), debe configurarse como una infraestructura de integridad que se sujeta a los siguientes principios y elementos esenciales:

- Ámbito de aplicación e inclusión**.** *"a) Permitir a todas las personas referidas en el artículo 3 comunicar información sobre las infracciones previstas en el artículo 2.".*

Implicaciones prácticas: El SII debe ser universal dentro del contexto laboral o profesional de la organización, incluso para determinadas personas que no formen parte de la misma. De este modo, debería garantizar el acceso a un amplio espectro de informantes, incluyendo no sólo a la plantilla, empleados, becarios, sino también a:

- Autónomos y profesionales independientes que trabajan para la misma.

- Personas que trabajan para proveedores o contratistas.

- Personas con relación profesional ya finalizada (extrabajadores, ex proveedores, etc.).

- Personas cuya relación profesional aún no ha comenzado (por ejemplo, personas en procesos de selección, aspirantes a colaborar profesionalmente).

Por otra parte, el SII debe permitir la recepción de todas las categorías de infracciones previstas en la ley (delitos penales, infracciones administrativas graves y muy graves, e infracciones del Derecho de la Unión Europea), sin perjuicio de que, al amparo de lo establecido en el artículo 7.4, puedan estar habilitados para recibir otras categorías de informaciones (ej. infracciones al código de conducta, etc.).

- Seguridad y confidencialidad. **"***b) Estar diseñado, establecido y gestionado de una forma segura, de modo que se garantice 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."*

Implicaciones prácticas: La confidencialidad del sistema interno de información es una garantía esencial para la protección efectiva de las personas informantes y para la validez y eficacia del propio sistema. Dicha confidencialidad debe integrarse en el diseño organizativo y funcional del sistema desde su origen.

A tal efecto, el sistema deberá operar mediante una plataforma segura y cifrada de extremo a extremo que impida la identificación directa o indirecta del informante, con accesos estrictamente restringidos y trazabilidad controlada, extendiéndose la confidencialidad no solo a la identidad de las personas implicadas, sino también al contenido de las comunicaciones y a cualquier dato que permita inferirla, y previniendo activamente usos indebidos del sistema o represalias de cualquier tipo.

- Principio de accesibilidad y omnicanalidad. "*c) Permitir la presentación de comunicaciones por escrito o verbalmente, o de ambos modos.*"

> **Implicación práctica**: El canal debe ofrecer una doble vía obligatoria:
>
> 1. **Por escrito**: Mediante formularios electrónicos seguros, correo postal o correo electrónico.
>
> 2. **Verbalmente**: Mediante línea telefónica o, si lo solicita el informante, mediante una reunión presencial con el Responsable del Sistema Interno de Información (RSII) en un plazo no superior a siete días.

- Principio de unificación y gestión centralizada. *"d) Integrar los distintos canales internos de información que pudieran establecerse dentro de la entidad."*

> **Implicación práctica**: Si la entidad posee múltiples buzones o canales de denuncia sectoriales que reciban comunicaciones del artículo 2 de la Ley 2/2023 (ej., Acoso Laboral, sexual, etc.), todos deben converger bajo la supervisión del RSII. El objetivo es ofrecer una "ventana única" de recepción de dichas informaciones, asegurando la aplicación uniforme de las garantías legales. En particular, la confidencialidad, seguridad, información al informante, plazos, etc.

- Efectividad y proactividad**.** *"e) Garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la correspondiente entidad u organismo con el objetivo de que el primero en conocer la posible irregularidad sea la propia entidad u organismo."*

> **Implicación práctica:** El procedimiento de gestión (Art. 9) debe ser ágil y eficaz garantizando tiempos de respuesta razonables, ausencia de represalias y una comunicación institucional inequívoca que refuerce la confianza en que las informaciones serán tratadas con seriedad, confidencialidad y neutralidad, favoreciendo la detección temprana y corrección interna de conductas irregulares, promoviendo así la autocorrección.

- Independencia funcional. *"f) Ser independientes y aparecer diferenciados respecto de los sistemas internos de información de otras entidades u organismos, sin perjuicio de lo establecido en los artículos 12 y 14."*

> **Implicación práctica**: Aunque la Ley permite la compartición de recursos del SII para ciertas entidades (Art. 12 para municipios pequeños y Art. 14 para entidades privadas de 50 a 249 trabajadores), la gestión y la responsabilidad final deben ser diferenciadas y la autonomía de cada SII debe preservarse.

El SII debe configurarse como un sistema propio, claramente identificable y no confundible con el de otras entidades u organismos con los que la organización se relacione o mantenga vínculos funcionales, estructurales o institucionales. En la práctica, ello exige su diferenciación respecto de entidades vinculadas o dependientes, estructuras territoriales o unidades con personalidad jurídica propia, así como de otros organismos, entes o grupos institucionales con sistemas de información autónomos.

Para ello, la página o portal de acceso al sistema deberá identificar de forma visible e inequívoca la entidad u organismo titular del sistema y delimitar su ámbito de aplicación, de modo que la persona informante conozca con claridad ante qué entidad está comunicando la información y bajo qué régimen de garantías será tratada.

- Liderazgo y responsabilidad**.** *"g) Contar con un responsable del sistema en los términos previstos en el artículo 8."*

Implicación práctica: La designación de un Responsable del Sistema Interno de Información (RSII) es obligatoria. Esta figura debe tener un estatus de independencia, autonomía y autoridad dentro de la entidad para ejercer sus funciones sin recibir instrucciones del órgano de administración o de otros directivos.

- Transparencia y divulgación. *"h) Contar con una política o estrategia que enuncie los principios generales en materia de Sistemas internos de información y defensa del informante y que sea debidamente publicitada en el seno de la entidad u organismo."*

Implicación práctica: Esta exigencia implica la aprobación de un documento formal que establezca los principios generales que rigen el funcionamiento del sistema, las garantías de confidencialidad, independencia y protección frente a represalias, así como los derechos y deberes de los informantes y afectados, así como de los que gestionan la información.

Dicha política deberá ser de fácil acceso y adecuadamente difundida con el fin de que todas las personas con una relación laboral o profesional con la entidad u organismo conozcan los canales disponibles, comprendan el alcance de la protección ofrecida y se genere la confianza necesaria para que la organización sea el primer ámbito al que se comuniquen posibles irregularidades.

- Debido proceso. *"i) Contar con un procedimiento de gestión de las informaciones recibidas."*

> **Implicación práctica**: Debe existir un protocolo de actuación escrito y formal que regule cada fase, desde el acuse de recibo hasta la conclusión y respuesta al informante, cumpliendo rigurosamente los plazos legales (7 días para el acuse; 3 meses para dar respuesta a las actuaciones), garantizando la confidencialidad de la identidad del informante y de las personas afectadas, la adecuada separación de funciones, la trazabilidad de las actuaciones y una gestión diligente, imparcial, evitando retrasos, interferencias o usos indebidos del sistema.

- Protección contra represalias. *"j) Establecer las garantías para la protección de los informantes en el ámbito de la propia entidad u organismo, respetando, en todo caso, lo dispuesto en el artículo 9."*

> **Implicación práctica**: La entidad debe incluir en su normativa interna (Reglamento del SII o Política) un compromiso y una lista de garantías que aseguren que el informante no sufrirá consecuencias negativas o represalias por haber comunicado de buena fe. Esto incluye la prohibición de acciones como el despido, el descenso de categoría, el traslado o cualquier acto discriminatorio con ocasión de la denuncia.

II.1.4. Externalización y compartición del SII (Arts. 6, 14 y 15 LPI)

- Externalización: La gestión del SII, puede ser externalizada a un tercero en los términos del artículo 6 de la Ley 2/2023. A estos efectos, se considera gestión del Sistema la recepción de informaciones.

  No obstante, la responsabilidad última por el correcto funcionamiento del Sistema y el cumplimiento de la Ley recae íntegramente en la entidad obligada. El RSII, aunque sea externo, debe cumplir los mismos requisitos de independencia.

  En el ámbito de la Administración General del Estado, Administraciones autonómicas y ciudades con Estatuto de Autonomía y en las Entidades que integran la Administración local, la gestión del sistema interno de información solo podrá externalizarse en los casos en que se acredite insuficiencia de medios propios, conforme a lo dispuesto en el artículo 116.4.f) de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público. Esta gestión comprenderá únicamente el procedimiento para la recepción de las informaciones sobre infracciones y, en todo caso, tendrá carácter exclusivamente instrumental.

- Compartición (sector público): La Ley permite que los municipios de menos de 10.000 habitantes puedan compartir el Sistema de Información y los recursos para la gestión, entre sí o con cualesquiera otras Administraciones públicas que se ubiquen dentro del territorio de la comunidad autónoma. También se admite esta posibilidad para aquellas

entidades del sector público con personalidad jurídica propia vinculadas o dependientes de órganos de las Administraciones territoriales con menos de 50 trabajadores, las cuales podrán compartir medios con la Administración de adscripción.

- Compartición (sector privado): Se permite que las entidades del sector privado que tengan entre 50 y 249 trabajadores compartan entre sí el SII y los recursos destinados a la gestión y tramitación de las comunicaciones, tanto si la gestión se lleva a cabo por cualquiera de ellas como si se ha externalizado, respetándose en todo caso las garantías previstas en la ley.

II.1.5. Grupos de Empresas (Art. 11 LPI)

La Ley 2/2023 configura la obligación de disponer de un Sistema Interno de Información (SII) como una obligación estrictamente individual. El artículo 10 determina que están obligadas las personas físicas o jurídicas del sector privado que tengan cincuenta o más trabajadores en España, así como aquellas incluidas en determinados sectores del Anexo. La pertenencia a un grupo de empresas no modifica esta regla: cada sociedad integrante debe analizar por sí misma si reúne los requisitos que la convierten en sujeto obligado, tal y como establece el artículo 11.

El primer inciso del artículo 11.1 atribuye a la sociedad dominante una función de dirección en materia de cumplimiento que comprende: a) aprobar una política general relativa al sistema interno de información a que se refiere el artículo 5 y a la defensa del informante, y b) asegurar la aplicación de los principios de esa política en todas las entidades que integran el grupo.

Esa política general debe respetar, sin embargo, dos límites expresamente mencionados en la propia norma:

1. La autonomía e independencia de cada sociedad, subgrupo o conjunto de sociedades integrantes, de acuerdo con el sistema de gobierno corporativo o de gobernanza del grupo.

2. La necesidad de introducir las modificaciones o adaptaciones necesarias para garantizar el cumplimiento de la normativa aplicable en cada caso.

Con todo, la norma sí que posibilitaría que el grupo de sociedades disponga de un único sistema interno de información operativo para todas las entidades que lo integran, si estas voluntariamente quieren sumarse a él, pero en el entendimiento de que la existencia de un sistema único no transforma al grupo en un único sujeto obligado ni altera la naturaleza individual de la obligación prevista en el artículo 10.

Implicación práctica: El hecho de que la sociedad matriz tenga su domicilio fuera de España no impide que el sistema interno de información sea único para todo el grupo, siempre que, respecto de la entidad obligada en España, dicho sistema se encuentre adaptado a la Ley 2/2023.

La normativa española no exige la existencia de un sistema "español" independiente, pero sí exige que el sistema utilizado por la entidad obligada cumpla íntegramente las condiciones materiales, procedimentales y organizativas previstas en la ley nacional. Si el sistema utilizado por la matriz no está configurado para cumplir estas exigencias, o si su diseño impide garantizar la autonomía operativa de la filial, entonces la entidad española no podrá utilizarlo como SII válido a efectos del cumplimiento del artículo 10.

II.2. El Responsable del Sistema Interno de Información (RSII)

La Ley 2/2023 (Art. 8) define la figura del Responsable del Sistema como la pieza clave para la gestión independiente de las comunicaciones.

II.2.1. Naturaleza del Responsable

El Responsable del Sistema puede ser:

- Persona física:

  En **sector privado,** el RSII será un directivo de la entidad, el cual ejercerá su cargo con independencia del órgano de administración o de gobierno de la misma.

  Cuando la naturaleza o la dimensión de las actividades de la entidad no justifiquen o permitan la existencia de un directivo Responsable del Sistema, será posible compatibilizar el desempeño ordinario de las funciones del puesto o cargo con las de RSII, tratando en todo caso de evitar posibles situaciones de conflicto de interés y garantizando siempre la ausencia de conflictos de interés y la total independencia en el ejercicio de su labor.

  En el sector público, el RSII debería ser designado entre empleados públicos, por ser quienes ofrecen mayores garantías de estabilidad, profesionalidad y sujeción al principio de legalidad. Cuando el responsable del sistema tenga la condición de directivo público, deberá garantizarse expresamente su independencia funcional en el ejercicio de esta función, asegurando un estricto cumplimiento del deber de confidencialidad, que no reciba instrucciones sobre la gestión concreta de las informaciones, y que exista una adecuada separación respecto de funciones decisorias, disciplinarias o sancionadoras. En la medida de lo posible, deberían excluirse de esta designación los cargos electos y los

responsables políticos, a fin de preservar la neutralidad del sistema, evitar interferencias partidistas y reforzar la confianza de las personas informantes.

Para ambos ámbitos, la Ley contempla que, si en las entidades u organismos obligados ya existiera una persona responsable de la función de cumplimiento normativo o de políticas de integridad, cualquiera que fuese su denominación, esta podrá asumir las funciones de RSII siempre que cumpla los requisitos establecidos en esta ley.

- Órgano colegiado:

La posibilidad de designar como RSII a un órgano colegiado puede ser útil en determinados casos para reforzar la confianza en el sistema, distribuir responsabilidades y reducir el riesgo de interferencias o instrumentalización. Asimismo, puede reducir el riesgo de interferencias o instrumentalización si integra perfiles complementarios, con experiencia jurídica, o de cumplimiento o de control interno.

> **Implicación práctica**: En estos casos, para ser operativo, el número de miembros no debería superar los cinco, debiendo siempre delegar en uno de ellos las facultades de gestión y tramitación de expedientes de investigación. No será exigible que todos ellos formen parte de la organización, pero en todo caso, el órgano debe contar con, al menos, un miembro interno de la entidad obligada. El órgano colegiado será el responsable del Sistema de dicha entidad, con independencia del origen de sus integrantes.

En el sector privado, cuando el RSII adopte la forma de órgano colegiado, la persona o entidad en quien dicho órgano delegue las funciones de gestión del sistema debería reunir los requisitos exigidos para el RSII en este ámbito, en los términos indicados anteriormente, ejerciendo sus funciones con plena independencia del órgano de administración o de gobierno y garantizando en todo caso la ausencia de conflictos de interés.

En el sector público, las garantías exigidas para cuando el RSII sea una persona física deberían ser observadas por todos los miembros del órgano colegiado, aunque de manera especialmente reforzada en la persona en quien se deleguen las funciones de gestión y tramitación del sistema. La condición de empleado público podrá dispensarse en uno de los miembros cuando resulte imprescindible recurrir a apoyo externo

II.2.2. Estatuto de Independencia y autonomía

- El RSII ejercerá sus funciones con plena independencia y autonomía respecto del resto de órganos de la entidad.
- No podrá recibir instrucciones de ningún tipo en el ejercicio de sus funciones.

- Debe disponer de todos los medios personales y materiales necesarios para llevar a cabo su labor.

II.2.3. Nombramiento y cese

La competencia para la designación del RSII y de su destitución o cese será del órgano de administración o de gobierno.

Tanto el nombramiento como el cese del RSII deben ser notificados a la Autoridad Independiente de Protección del Informante (A.A.I.) o, en su caso, a las autoridades u órganos competentes de las Comunidades Autónomas, en el plazo de diez días hábiles, especificando, en el caso del cese, las razones que han justificado el mismo.

No obstante lo anterior, la Disposición Transitoria Única. 4, del Estatuto de la Autoridad Independiente de Protección del Informante, A.A.I., aprobado por Real Decreto 1101/2024, de 29 de octubre, establece un plazo de dos meses para comunicar el nombramiento del Responsable del Sistema interno de información.

A estos efectos, dicho plazo comenzará a computarse desde el momento en que se publique en el portal web de la AIPI (www.proteccioninformante.gob.es) el formulario específico de notificación del responsable del canal interno.

II.2.4. Grupos de empresas

El artículo 11.2 establece que el RSII podrá ser uno para todo el grupo, o bien uno para cada sociedad integrante del mismo, subgrupo o conjunto de sociedades, en los términos que se establezcan en la política general aprobada por la dominante.

El primero de los supuestos debería tener en cuenta que:

- La obligación de disponer de un sistema interno de información seguiría recayendo individualmente sobre cada sociedad obligada.
- En este supuesto no estaríamos hablando de un “Responsable único del sistema del grupo” como sujeto abstracto, sino que se permite que la misma estructura personal u orgánica asuma la condición de responsable respecto de varias sociedades, designada y comunicada en los términos de la ley. Cada sociedad tiene su propio responsable, pero, en este caso, sería la misma persona para las diversas sociedades del grupo.
- Será necesario un acuerdo expreso de la entidad obligada designando al RSII.

Por su parte, cuando las sociedades del grupo no compartan un mismo sistema interno de información, resulta recomendable que el responsable del sistema designado para cada entidad tenga la condición de directivo de la sociedad obligada, a fin de garantizar un

conocimiento suficiente de su organización, una adecuada capacidad de actuación y el ejercicio efectivo de la independencia funcional a que se refiere el artículo 11 de la Ley 2/2023.

II.3. Características mínimas de diseño del canal interno de información (CII)

El Canal Interno de Información (CII) es el punto de entrada de las comunicaciones y debe estar diseñado para cumplir con los requisitos de accesibilidad, seguridad y documentación que establece la Ley.

II.3.1. Principios de diseño y estructura

Requisito	Descripción Mínima	Fundamento Legal
1. Integración Obligatoria	El canal debe estar formalmente integrado dentro de la estructura general del **Sistema Interno de Información (SII** (Art. 5).	Art. 7.1
2. Accesibilidad Universal	Debe permitir la comunicación a **todas las personas** contempladas en el ámbito subjetivo de la Ley (trabajadores, extrabajadores, contratistas, etc.).	Art. 7.1, en conexión con Art. 3
3. Admisión del Anonimato	El diseño técnico del canal **debe permitir** la presentación y la posterior tramitación de comunicaciones anónimas.	Art. 7.3
4. Contenido	El canal puede estar habilitado para recibir otras comunicaciones ej. infracciones del código de conducta, actuaciones que sin ser delito ni infracciones administrativas graves o muy graves supongan o amparen actuaciones fraudulentas, etc. pero debe advertirse claramente que estas quedan **fuera del ámbito de protección** de la Ley.	Art. 7.4

II.3.2. Vías de comunicación

El **artículo 7.2** de la Ley 2/2023 (en relación con el 5.2.c) establece que el **canal interno** permitirá realizar comunicaciones *'por escrito o verbalmente, o de las dos formas'*. No obstante, como buena práctica para maximizar la eficacia del canal, **se recomienda que éste soporte ambos métodos de entrada.**

Vías escritas:

- Correo Postal: Permitiendo la remisión de documentos físicos.
- Medios Electrónicos Habilitados: Plataforma de software seguro, formularios web o correo electrónico dedicado.

- Vías verbales:

- Vía Telefónica: Línea dedicada para la recepción de informaciones verbales.
- Sistema de Mensajería de Voz: Sistemas que permitan la grabación o transcripción de mensajes de audio.
- Reunión Presencial (a solicitud del informante): El informante tiene derecho a solicitar una reunión presencial con el Responsable del Sistema Interno de Información (RSII). Esta debe llevarse a cabo en un plazo máximo de siete días desde la solicitud.

II.3.3. Requisitos de contenido y documentación

La ley impone rigurosos requisitos de documentación, especialmente para las comunicaciones verbales, y de advertencias al informante:

- Documentación de comunicaciones verbales (Exclusivo Art. 7.2)

La documentación de las comunicaciones verbales (teléfono, voz o presencial) es obligatoria y se debe realizar previo consentimiento del informante, a través de una de estas dos formas:

1. Mediante grabación: Registrar la conversación en un formato seguro, duradero y accesible.

2. Mediante transcripción: Elaborar una transcripción completa y exacta de la conversación por el personal responsable.

Garantía del Informante: Si se opta por la transcripción, se debe ofrecer al informante la oportunidad de comprobar, rectificar y aceptar la transcripción mediante su firma, respetando sus derechos de protección de datos.

- Información y advertencias obligatorias

El sistema debe garantizar que se cumple con la obligación de informar al comunicante sobre:

- Tratamiento y protección de datos: Advertencia de que la comunicación será grabada (si aplica) y la información sobre el tratamiento de sus datos personales conforme al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento general de protección de datos, RGPD).
- Notificación segura: La posibilidad de que el informante pueda indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones oficiales.
- Canales externos: Información clara y accesible sobre la existencia de los canales externos de información ante las Autoridades Competentes (como la Autoridad Independiente de Protección del Informante o las Autoridades Autonómicas) y, en su caso, ante las instituciones de la Unión Europea.

II.3.4 Conexión con el Libro-Registro (Art. 26 LPI)

El canal interno es la fuente primaria de datos para el Libro-Registro de las Informaciones, cuya llevanza es obligatoria para la entidad (ya sea pública o privada).

- Función del canal: El CII actúa como la "puerta de entrada" que genera la información necesaria para el registro.
- Obligación de registro (Art. 26): Todas las comunicaciones recibidas a través del canal, así como las investigaciones internas, deben ser registradas en un libro-registro seguro, garantizando la confidencialidad y el acceso restringido.
- Datos clave a registrar: El registro debe contener, al menos, la fecha de recepción de la información, el objeto de la comunicación, el estado de las actuaciones (en curso, archivado, resolución) y la fecha de finalización del procedimiento, asegurando la trazabilidad de cada caso.

II.4. Procedimiento de gestión de información: obligaciones

El artículo 9 establece los principios y garantías mínimas que debe tener el procedimiento de gestión de informaciones.

II.4.1 Principios generales del procedimiento (Art. 9.1 LPI)

- Respeto al principio de presunción de inocencia: Garantía fundamental para cualquier persona afectada o mencionada en la comunicación.

- Protección del honor: Protección de la reputación de la persona afectada.
- Confidencialidad: La gestión debe ser segura y garantizar la reserva de la identidad del informante y de la persona afectada.
- Protección de datos: Cumplimiento estricto del Reglamento General de Protección de Datos y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Imparcialidad y objetividad.
- Diligencia y celeridad.

II.4.2 Obligaciones mínimas del procedimiento (Art. 9.2 LPI)

Las siguientes obligaciones definen las fases clave y los requisitos temporales del proceso:

Literal	Obligación Legal	Conexión y Finalidad
a)	**Identificación del Canal(es)**: Identificación del canal o canales internos a los que se asocia el procedimiento.	Requisito de claridad para el **SII**, asegurando que el procedimiento aplica a las vías correctas de recepción.
b)	**Información de Canales Externos**: Incluir información clara y accesible sobre el uso de canales externos ante las autoridades competentes (AAI) y, en su caso, ante las instituciones de la Unión Europea.	Es un requisito de transparencia del **CII** que el **RSII** debe garantizar en la documentación.
c)	**Acuse de Recibo**: Envío de acuse de recibo al informante en un plazo de **siete días naturales** siguientes a la recepción. *Excepción:* No se envía si pone en peligro la confidencialidad.	Primera acción temporal del **RSII** que marca el inicio de la trazabilidad del expediente.
d)	**Plazo Máximo para dar respuesta**: Determinación del plazo máximo de **tres meses** (ampliable a seis meses en casos de especial complejidad). El plazo de tres meses se cuenta desde la recepción o desde el vencimiento del plazo de siete días (si no se remitió acuse).	El **RSII** es el responsable de la gestión temporal y debe notificar al informante la prórroga si aplica.
e)	**Mantener la Comunicación**: Prever la posibilidad de comunicación segura con el informante y solicitarle información adicional para la instrucción.	Requisito funcional del **CII** para apoyar la fase de **Instrucción y Comprobación**.
f)	**Derecho de Audiencia y Defensa**: Informar a la persona afectada de los hechos que se le atribuyen y garantizar su derecho a ser oída. La comunicación	Garantía procesal esencial que el **RSII** debe gestionar de forma imparcial.

	debe hacerse en tiempo y forma adecuados para no frustrar la investigación.	
g)	**Confidencialidad en la tramitación y remisión**: Establecer la obligación del personal no responsable (que reciba por error la comunicación) de remitirla inmediatamente al **RSII** y de mantener la confidencialidad.	Requisito organizativo fundamental para proteger la identidad desde el momento inicial.
h)	**Respeto a Garantías**: Exigencia del respeto a la **presunción de inocencia** y al **honor** de las personas afectadas.	Principio rector que debe guiar las actuaciones del **RSII** durante toda la instrucción.
i)	**Protección de Datos Personales**	Respeto a las disposiciones sobre protección de datos de acuerdo con lo previsto en el Título VI de la Ley.
j)	**Remisión a Fiscalía**: Remisión de la información al **Ministerio Fiscal** con carácter inmediato cuando los hechos sean indiciariamente constitutivos de delito. Si afecta a intereses UE, se remitirá a la **Fiscalía Europea**.	Salida obligatoria del procedimiento que el **RSII** debe ejecutar sin dilación.

III. LISTA DE VERIFICACIÓN BÁSICA PARA EL DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA INTERNO DE INFORMACIÓN

- ☐ Consulta previa a la representación sindical.
- ☐ Acuerdo del Órgano de Gobierno aprobando el Sistema y la Política.
- ☐ Designación formal del Responsable del Sistema (RSII).
- ☐ Notificación del nombramiento a la AIPI/Autoridad autonómica.
- ☐ Implementación técnica del Canal (Software/Buzón seguro).
- ☐ Aprobación del Procedimiento de Gestión de Informaciones.
- ☐ Publicidad del canal en la página web (acceso visible y fácil).
- ☐ Formación al personal sobre el uso del canal.

Autoridad Independiente
de Protección del Informante