Autoridad Independiente
de Protección del Informante

Recomendación

1/2025 de la Autoridad Independiente de Protección del Informante

para la gestión del Sistema Interno de Información en los partidos políticos (v3)

Madrid, enero de 2026

Autoridad Independiente
de Protección del Informante

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 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, de 20 de febrero, 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".*

Los partidos políticos, en su calidad de sujetos obligados por el artículo 10.1.b) de la Ley, desempeñan un papel fundamental en nuestro sistema democrático y, dada su relevancia constitucional y la percepción pública a la que están expuestos, requieren de unos estándares de integridad y transparencia especialmente reforzados. No obstante, esta Autoridad es consciente de las singularidades organizativas de estas entidades y de los riesgos específicos inherentes a su dinámica interna. En particular, resulta prioritario evitar disfuncionalidades en la aplicación de la norma que pudieran derivar en un uso instrumental de los canales de denuncia, desvirtuando su finalidad preventiva para convertirlos en herramientas de conflicto interno.

En este contexto, el objeto específico de esta Recomendación es orientar el cumplimiento de las obligaciones contenidas en la Ley 2/2023, de 20 de febrero, a los partidos políticos, todo ello sin perjuicio de las competencias que puedan tener, en su caso, las autoridades autonómicas de protección del informante. El objetivo es adaptar las exigencias de la Ley 2/2023 a la naturaleza específica de estas organizaciones, garantizando que el Sistema Interno de Información (SII) sirva al fortalecimiento institucional y no sea objeto de instrumentalización para fines ajenos a los previstos en la norma.

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

Recomendación AIPI 1/2025 (v3) para la gestión del Sistema Interno de Información en los partidos políticos

I. OBJETIVO Y DESTINATARIOS

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, contiene en su título II el régimen jurídico del Sistema Interno de información, que se configura como el cauce preferente para informar sobre las acciones u omisiones previstas en el artículo 2 de la Ley, siempre que se pueda tratar de manera efectiva la infracción y si el denunciante considera que no hay riesgo de represalia.

El Sistema Interno de Información, que abarca tanto el canal –entendido como buzón o cauce para recepción de la información– como el Responsable del Sistema y el procedimiento, se configura en la Ley como el medio preferente para canalizar la información, pues una actuación diligente y eficaz en el seno de la propia organización podría paralizar las consecuencias perjudiciales de las actuaciones investigadas.

Con relación al sector público, la Ley extiende con toda su amplitud la obligación de contar con un Sistema Interno de Información, estableciendo la obligación de configuración del Sistema a entidades públicas y del sector privado.

Concretamente, el artículo 10 establece que, en el caso del sector privado,

> *1. Estarán obligadas a disponer de un Sistema interno de información en los términos previstos en esta ley:*
>
> *a) Las personas físicas o jurídicas del sector privado que tengan contratados cincuenta o más trabajadores.*
>
> *b) 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 será de aplicación en lo no regulado por su normativa específica.*
>
> *Se considerarán 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) **Los partidos políticos**, los sindicatos, las organizaciones empresariales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos.*
>
> *2. Las personas jurídicas del sector privado que no estén vinculadas por la obligación impuesta en el apartado 1 podrán establecer su propio Sistema interno de información, que deberá cumplir, en todo caso, los requisitos previstos en esta ley.*

El objeto específico de esta Recomendación es orientar el cumplimiento de las obligaciones contenidas en la Ley 2/2023, de 20 de febrero, a los **partidos políticos**, todo ello sin perjuicio de las competencias que puedan tener, en su caso, las autoridades autonómicas de protección del informante. El objetivo es adaptar las exigencias de la Ley 2/2023 a la naturaleza específica de estas organizaciones, garantizando que el Sistema Interno de Información (SII) sea un baluarte de integridad y no un instrumento de confrontación política.

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

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, contiene en su título II el régimen jurídico del Sistema Interno de información, que se configura como el cauce preferente para informar sobre las acciones u omisiones previstas en el artículo 2 de la Ley, siempre que se pueda tratar de manera efectiva la infracción y si el denunciante considera que no hay riesgo de represalia.

El Sistema Interno de Información (SII), que abarca tanto el canal –entendido como buzón o cauce para recepción de la información– como el Responsable del Sistema y el procedimiento, se configura en la Ley como el medio preferente para canalizar la información, pues una actuación diligente y eficaz en el seno de la propia organización podría paralizar o reducir las consecuencias perjudiciales de las actuaciones investigadas.

La Ley 2/2023 impone la obligación de disponer de un SII a partidos políticos **con independencia del número de trabajadores**, lo que los diferencia del régimen general aplicable a otras entidades privadas (que solo están obligadas si tienen 50 o más empleados).

Esta singularidad normativa tiene su fundamento en el singular papel constitucional que tienen estas organizaciones (art. 6 CE) como manifestación del pluralismo político, la voluntad popular y, en definitiva, instrumento fundamental para la participación política.

La propia ley reconoce, en su exposición de motivos, que los partidos políticos, como entidades de relevancia constitucional y piezas clave del sistema democrático, están sujetos a una exposición de riesgo singular. En este contexto, el sistema interno de información se convierte en un mecanismo esencial para garantizar la transparencia y la integridad en

instituciones que son pilares del sistema democrático y de las que se exige una actitud ejemplar.

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

El Sistema Interno de Información (SII) 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 (art. 10.c)

Los **partidos políticos, los sindicatos, las organizaciones empresariales y las fundaciones** creadas por unos y otros, siempre que reciban o gestionen fondos públicos, independientemente del número de empleados que tengan.

II.1.2. Consulta y aprobación (art. 5.1)

Para la implantación del Sistema, se requiere la consulta previa a los representantes sindicales y/o a la representación legal de las personas trabajadoras (delegados o Comité de empresa, dependiendo del número de trabajadores) de la organización que se trate. De acuerdo con el artículo 64 del Estatuto de los trabajadores por consulta se entiende el intercambio de opiniones y la apertura de un diálogo entre el empresario y el comité de empresa sobre una cuestión determinada, incluyendo, en su caso, la emisión de informe previo por parte del mismo; Incluimos la representación sindical porque la Ley Orgánica de Libertad Sindical (art. 10.3) establece las mismas garantías para los delegados sindicales, los miembros del comité de empresa y los delegados de personal (las recogidas en el art. 68 ET y concordantes).

La aprobación final corresponde al órgano de gobierno o equivalente de la entidad, quien es el responsable último de su implantación.

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

El SII, 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 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 (por ejemplo, asesores externos, consultores de comunicación, abogados, economistas o auditores, etc.).

- Personas que trabajan para proveedores o contratistas del partido (por ejemplo, empleados de empresas de marketing electoral, de eventos, de comunicación o logística, de empresas tecnológicas que gestionan datos o campañas, etc.).

- Personas con relación profesional ya finalizada (por ejemplo, exasesores, extrabajadores, ex proveedores).

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

- Personas vinculadas a entidades del entorno del partido (por ejemplo, personal de fundaciones vinculadas al partido, personal de asociaciones que ejecutan proyectos financiados por el partido si existe conexión funcional real).

- La condición de militante de un partido político, aun cuando implique el pago de cuotas, la participación en asambleas o el ejercicio de derechos estatutarios, no constituye por sí misma una relación laboral o profesional en los términos exigidos por la Ley 2/2023. En consecuencia, las comunicaciones formuladas exclusivamente desde la posición de militancia, así como las eventuales medidas estatutarias que pudieran adoptarse en ese ámbito, no quedan comprendidas en el ámbito subjetivo de aplicación de la citada Ley, en la que el régimen de protección del informante se vincula estrictamente a la existencia de un contexto laboral o profesional.

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.).

Todo ello se entiende sin perjuicio de que los propios partidos puedan establecer otros cauces internos de garantía, control o impugnación, diseñados al efecto dentro del marco de los estatutos del partido, los cuales no tendrían que someterse a los requisitos ni a las garantías que establece la Ley 2/2023.

- Seguridad, 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**: En el ámbito de un partido político, la garantía de confidencialidad del sistema interno de información constituye un elemento estructural esencial para la protección efectiva de las personas informantes y una condición indispensable para la validez, eficacia y legitimidad del sistema interno de información del partido, habida cuenta de los riesgos específicos derivados de la organización política, la pluralidad de corrientes internas y la especial exposición a represalias directas o indirectas.
>
> Dicha garantía no se agota en la adopción de medidas técnicas de seguridad, sino que debe integrarse en el diseño organizativo y funcional del sistema desde su origen. En particular:
>
> - El sistema deberá articularse mediante una plataforma segura, cifrada de extremo a extremo, que permita la presentación de comunicaciones desde el primer momento a través de un canal que no posibilite la identificación directa o indirecta de la identidad del informante y que disponga de un registro de accesos y actuaciones (trazabilidad controlada).
>
> - Deberán implantarse medidas organizativas que aseguren que únicamente las personas expresamente habilitadas para la gestión del sistema tengan acceso a la información, quedando excluido cualquier acceso por razón de cargo orgánico, responsabilidad política, jerarquía interna o pertenencia a órganos de dirección.
>
> - La confidencialidad debe extenderse no solo a la identidad del informante y de las personas afectadas, sino también al contenido de las comunicaciones y a cualquier dato o circunstancia que permita inferir dicha identidad.
>
> - Debería prevenirse activamente la circulación informal de información, la utilización del sistema con fines políticos o disciplinarios indebidos y cualquier forma de represalia directa o indirecta.

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

> **Implicaciones prácticas**: 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.

La exigencia de que el Sistema Interno de Información permita la presentación de comunicaciones de forma verbal debe entenderse referida al canal y no a la solución tecnológica asociada en cada caso. En consecuencia, resulta conforme con la Directiva (UE) 2019/1937 y con la Ley 2/2023 que el software no soporte llamadas telefónicas, siempre que el Sistema Interno de Información garantice efectivamente una vía verbal –por ejemplo, mediante una línea telefónica dedicada gestionada por el Responsable del Sistema– y permita, a solicitud del informante, la celebración de una reunión presencial dentro del plazo legalmente previsto.

El artículo 5.2.c) de la Ley 2/2023 debe interpretarse en el sentido de que los canales de denuncia han de permitir la presentación de comunicaciones tanto por escrito como verbalmente.

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

Implicaciones prácticas: 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 tener una gestión con garantías unificadas y bajo un mismo responsable del sistema.

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.

En definitiva, la Ley 2/2023 exige que el Sistema Interno de Información pueda recibir todas las comunicaciones relativas a las infracciones previstas en su artículo 2. Esta exigencia no implica la supresión de canales específicos derivados de la negociación colectiva o de normativa sectorial –como los vinculados a la prevención del acoso– sino tan sólo la integración funcional y organizativa en el SII de aquellos que estén concebidos para comunicar tales infracciones, previa acomodación a las garantías establecidas en la Ley 2/2023.

- 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."*

Implicaciones prácticas: 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, evitando su instrumentalización política y 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."*

Implicaciones prácticas: El SII del partido debe ser un sistema propio, identificable y no confundible con el de otras entidades con las que el partido se relaciona o que orbitan alrededor suyo. En la práctica implica:

- Separación respecto a fundaciones y asociaciones vinculadas.
- Separación respecto a estructuras territoriales con personalidad propia (por ejemplo, si hay federaciones/organizaciones territoriales o locales jurídicamente distintas).
- Separación respecto a grupos institucionales (el canal del partido no debe confundirse con el del grupo parlamentario o el de una administración).

Lo anterior exige que en la página / portal de internet del canal debe constar de forma visible qué entidad es la titular del sistema y el ámbito a que se proyecta, para que el informante sepa dónde está denunciando y con qué garantías.

- 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. Esta exigencia cobra especial intensidad en el seno de los partidos políticos, por tener rasgos específicos que no aparecen con tanta intensidad en empresas ordinarias (por ejemplo, politización, conflictos internos). Más adelante nos ocuparemos de ellos de forma singularizada.

- 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: En el ámbito de los partidos políticos, la exigencia de contar con una política o estrategia en materia de sistemas internos de información y defensa del informante 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 las personas informantes y de quienes gestionan el sistema.

Dicha política debe ser de fácil acceso (por ejemplo, intranet, tablones, web pública) para que todas las personas con una relación laboral o profesional con la organización conozcan sus derechos y los canales disponibles y así generar confianza en el sistema y favorecer que el partido 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 la resolución), garantizando la confidencialidad de la identidad del informante y de las personas afectadas, la separación entre la gestión de la información y cualquier decisión política u orgánica, así como la trazabilidad de las actuaciones realizadas, evitando retrasos, interferencias o usos indebidos del sistema y asegurando una respuesta diligente, neutral y conforme a Derecho.

- 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.2. 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.2.1. 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. A estos efectos será de aplicación lo establecido en el II.1.3 anterior, cuando se refiere al ámbito de aplicación e inclusión.	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.2.2. Vías de comunicación

El **artículo 7.2** de la Ley 2/2023 (en relación con el art. 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, **nuestro criterio es que éste debe soportar ambos métodos de entrada, como ya indicamos.**

- **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.2.3. 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.2.4. Conexión con el Libro-Registro (art. 26)

El canal interno es la fuente primaria de datos para el Libro-Registro de las Informaciones, cuya llevanza es obligatoria para la entidad.

- 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.3. 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.3.1. Principios generales del procedimiento (art. 9.1)

- 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.3.2. Obligaciones mínimas del procedimiento (art. 9.2)

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)	**Inclusión en el registro con número de entrada y 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 y a la confidencialidad. La comunicación debe hacerse en tiempo y forma adecuados para no frustrar la investigación.	Garantía procesal esencial que el **RSII** debe gestionar de forma imparcial.
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 la 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.

II.4. El Responsable del Sistema (RSII): Prestigio, proximidad y garantía

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.4.1. Naturaleza del responsable

El responsable del Sistema puede ser:

- Persona física: Un directivo de la entidad.
- Órgano colegiado: En caso de optar por un órgano colegiado (ej. Comité de Cumplimiento), este deberá delegar en uno de sus miembros las facultades de gestión y tramitación de expedientes de investigación.
- Compatibilidad de funciones: Si ya existe en la entidad una persona responsable de la función de cumplimiento normativo (*Compliance Officer*) o de políticas de integridad, podrá ser designada RSII, siempre que cumpla estrictamente con los requisitos de independencia y autonomía establecidos.

II.4.2. 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.4.3. Nombramiento y cese

La competencia para la designación del Responsable del Sistema, y de su destitución o cese será el órgano de administración de gobierno. En los partidos políticos para garantizar su

independencia y dar credibilidad al sistema, debería establecerse previamente un plazo determinado para el mandato, y fijar previamente unas causas de cese tasadas.

Tanto el nombramiento como el cese del RSII de los partidos políticos de ámbito nacional deben ser notificados a la Autoridad Independiente de Protección del Informante (A.A.I.) en el plazo de diez días hábiles.

La misma exigencia será de aplicación para los partidos cuyo ámbito supere el territorio de una comunidad autónoma, así como a aquellos que, aun teniendo un ámbito limitado a una sola comunidad autónoma, en la misma no exista autoridad autonómica con competencias sancionadoras en materia de protección del informante en el sector privado, conforme a lo previsto en el Título IX de la Ley 2/2023. El cese, en todo caso, debe estar justificado y notificarse a la Autoridad con las razones del mismo

Para el resto de partidos políticos que no tengan ámbito nacional se recomienda que, además de a su autoridad autonómica, también remitan el nombramiento y cese a la AIPI, a efectos de asegurar una base de datos nacional que cumpla con los requisitos de seguimiento y control de implementación de la Directiva por parte de la Unión Europea.

La Disposición Transitoria Única, del Estatuto de la Autoridad Independiente de Protección del Informante, A.A.I., aprobado por Real Decreto 1101/2024, de 29 de octubre, en su apartado 4, establece un plazo de dos meses para comunicar el nombramiento del Responsable del Sistema interno de información. No obstante, 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.4.4. Recomendaciones específicas para los partidos políticos

Para garantizar la eficacia del sistema, para la designación del Responsable del Sistema Interno de Información (RSII) deberían garantizarse los siguientes principios:

1. **Garantizar la independencia real (no sólo formal).** El objetivo es blindar su autonomía y evitar conflictos de interés en la toma de decisiones. En un partido político esto implica:

    - Evitar cargos orgánicos de dirección política (secretarías generales, ejecutivas, direcciones de campaña). Se recomienda que el RSII no forme parte de los órganos ejecutivos del partido ni de su "parlamento interno" (comités federales, juntas directivas, etc.).
    - Evitar perfiles “orgánicamente contaminados”, personas directamente subordinadas respecto de los anteriores, miembros de órganos disciplinarios del partido, responsables de recursos humanos internos.
    - Priorizar perfiles que no participen en decisiones estratégicas ni disciplinarias.

2. **Exigir formación jurídica específica, no solo confianza política**. El RSII debería contar con formación acreditable o experiencia previa en compliance, auditoría, derecho público o penal económico. Podría ser el antiguo *Compliance Officer* o responsable de integridad, siendo imperativo que cuente con a*uctoritas o* liderazgo ético. prestigio profesional, autoridad moral, formación y conocimiento en la materia. Esto se traduce en un reconocimiento interno basado en su trayectoria, integridad y competencia técnica. No es solo "saber", sino ser percibido como una figura cuya opinión e independencia son incuestionables para todos los estamentos del partido.

3. **Referente de Confianza y Proximidad.** El RSII debe ser percibido como el principal aliado de los trabajadores y personal de la entidad. Su función no es solo de vigilancia, sino de acompañamiento y protección. Es la figura a la que cualquier empleado puede acudir sabiendo que será escuchado con empatía, que su identidad estará blindada y que su bienestar profesional es la prioridad del sistema.

4. **Órganos Colegiados.** En organizaciones de alta complejidad como los partidos, se recomienda que el RSII sea un órgano colegiado, en la medida que ello puede generar mayor confianza interna, reparte la responsabilidad, dificulta interferencias directas y reduce el riesgo de instrumentalización personal, sobre todo cuando integra perfiles complementarios (p. ej. un perfil jurídico, otro de compliance/auditoría, y otro externo o independiente.

   No deberá exceder de 5 miembros para garantizar agilidad. El órgano colegiado será el responsable del Sistema de dicha entidad, con independencia del origen de sus integrantes. No será exigible que todos sus miembros 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 deberá delegar en uno de sus miembros las facultades de gestión del Sistema interno de información y de tramitación de expedientes de investigación.

   La operatividad en el funcionamiento del órgano hace que en estos casos sea conveniente que se establezcan:

   - Reglas estrictas de confidencialidad: compromisos individuales firmados, reglas de acceso restringido a la información, etc.)
   - Reglas para abordar conflictos de intereses, abstenciones y sustituciones: debe estar previsto cuándo un miembro se abstiene, quién lo sustituye, cómo se documenta, etc.

5. **No delegación:** Si bien el artículo 6 de la Ley permite la gestión externa del canal (apoyo técnico), es decir, que la titularidad del RSII puede externalizarse para la gestión de información, la responsabilidad no puede nunca delegarse. El responsable (persona u órgano) debe ejercer de forma efectiva, prohibiéndose el uso de figuras interpuestas.

II.5. El SII como salvaguarda frente al riesgo reputacional

Los partidos políticos operan bajo la "teoría del riesgo extremo" debido a su exposición pública y la competencia electoral. Por ello:

1. **Detección precoz**: El sistema debe estar diseñado para identificar conductas de riesgo en momentos críticos (procesos electorales, licitaciones públicas, nombramientos).
2. **Instrumento de prevención:** El SII y sus canales no deben convertirse en herramientas de activismo o lucha política interna. Su utilización para fines distintos a los previstos en la norma desnaturaliza o desvirtúa el espíritu de la Ley y de la Directiva, cuyo fin exclusivo es aflorar irregularidades y proteger al informante.
3. **Uso del canal y confianza:** Un canal bien gestionado protege la reputación del partido. Un mal uso genera un daño devastador no solo en el ámbito laboral, sino en la percepción de los militantes y el electorado.

II.6. Garantías de protección y transparencia

1. **Protección Integral:** La protección frente a represalias debe extenderse no solo al informante, sino de manera específica al **RSII y su equipo**, evitando cualquier medida discriminatoria o disciplinaria derivada del ejercicio de sus funciones de investigación.
2. **Reporte Continuo:** El RSII tiene el deber de reportar con frecuencia periódica a los órganos del partido (sin vulnerar la confidencialidad de los expedientes), informando sobre métricas, salud del sistema y propuestas de mejora de los códigos éticos preexistentes.
3. **Aprovechamiento del *Compliance*:** Los partidos deben integrar en el SII toda la experiencia previa de sus modelos de cumplimiento y códigos éticos, evitando duplicidades y fomentando una cultura de integridad única.

III. CONCLUSIONES PARA LA IMPLEMENTACIÓN

- **Externalización sensata:** El apoyo de terceros externos es una solución válida para aportar imparcialidad, siempre que se vigilen estrictamente los conflictos de interés de dichos proveedores con la propia organización política.
- **Neutralidad técnica:** El SII debe ser percibido como una "zona neutral" dentro del partido, gestionada con criterios técnicos y jurídicos, alejada de las dinámicas de poder orgánico.
- El RSII es el puente de confianza que une la base de la organización con su cúpula directiva. Su misión es doble: ser el **protector máximo del informante** y el **estratega**

ético que reporta a la dirección para blindar al partido contra la corrupción y el descrédito.

- **Aplicación supletoria** de las previsiones de la Ley 2/2023 para el canal externo a la gestión de los canales internos de los partidos, en todo aquello que sea compatible con su estructura orgánica y funciones constitucionales.
- Dada la naturaleza de los partidos, el sistema debe estar especialmente calibrado para detectar riesgos en tiempos y conductas críticas. El RSII, apoyándose en la **experiencia de *compliance* previa**, debe monitorizar los momentos de mayor vulnerabilidad ética para la organización, actuando como un consultor preventivo más que como un mero sistema sancionador.

Autoridad Independiente
de Protección del Informante