

Nota sobre la Recomendación 1/2026 de la AIPI para el diseño e implementación del SII

La Autoridad Independiente de Protección del Informante (AIPI) ha publicado recientemente la [Recomendación 1/2026](#), relativa al diseño e implementación de los Sistemas Internos de Información (SII) previstos en la Ley 2/2023.

Sin perjuicio de que la Recomendación no tenga carácter normativo, esta fija criterios interpretativos y estándares técnicos prácticos a tomar en consideración por la AIPI en su condición de entidad con atribuciones de supervisión y sancionadoras en materia de Sistemas internos de información, motivo por el que resulta de gran importancia, motivo por el que procedemos a través de la presente circular a destacar las principales recomendaciones realizadas por la AIPI:

- **Computo de personas trabajadoras:** Para determinar si una empresa alcanza el umbral de 50 o más trabajadores (cuestión de gran importancia para determinar el ámbito de aplicación en el sector privado), la AIPI utiliza el criterio del artículo 3 del Real Decreto 901/2020 de 13 de octubre por el que se regulan los planes de igualdad. En atención a esta disposición normativa, computarán como trabajadores, cualquier persona empleada con una relación laboral, incluyendo fijos discontinuos, contratos de duración determinada y también de puesta a disposición (ETT). Los trabajadores a tiempo parcial contarán como “una persona más” y en el caso de trabajadores de duración determinada, deberán computarse los contratos extinguidos en los seis meses anteriores al momento del computo; cada 100 días se computará como una persona trabajadora más.

El cómputo debe realizarse, al menos, el último día de los meses de junio y diciembre de cada año.

- La AIPI subraya que el Sistema Interno de Información no puede concebirse como un mero buzón de denuncias, sino como una **infraestructura básica de gobernanza ética**, clarificando varias cuestiones prácticas, de las que destacamos las siguientes:
 - Aprobación: La aprobación del Sistema exige, con carácter previo, la consulta a la representación legal de las personas trabajadoras y, en todo caso, su aprobación formal por el órgano de administración o de gobierno, junto con la correspondiente política del sistema y designación del Responsable del Sistema interno de información.
 - El sistema debe tener un ámbito de aplicación universal, accesible a todas las personas que mantengan o hayan mantenido una relación laboral o profesional con la entidad (empleados, extrabajadores, proveedores, contratistas, profesionales independientes o candidatos) y permitir la recepción de todas las infracciones previstas en la Ley 2/2023. Asimismo, el SII podrá habilitarse para otras comunicaciones (como infracciones del código de conducta u otras irregularidades internas que, sin constituir delito ni infracción administrativa grave o muy grave, supongan o amparen actuaciones fraudulentas), si bien deberá advertirse de forma clara y expresa que dichas comunicaciones quedan fuera del ámbito específico de protección previsto en la Ley 2/2023.
 - El SII deberá garantizar confidencialidad y seguridad, operando a través de una plataforma segura y cifrada de extremo a extremo, con accesos restringidos y trazabilidad controlada, extendiendo la confidencialidad a la identidad de las personas implicadas, al contenido de

las comunicaciones y a cualquier dato que permita inferirla, y adoptando medidas activas frente a usos indebidos o represalias¹.

- El SII deberá garantizar la accesibilidad efectiva mediante un enfoque de omnicanalidad, estableciendo la obligación de ofrecer una doble vía de comunicación y -respecto a las plataformas de comunicación segura- se recomienda que permitan la presentación de comunicaciones tanto por escrito como de forma verbal.
- Unificación y gestión centralizada: En aquellos casos en los que coexistan buzones o canales sectoriales de denuncia que reciban comunicaciones comprendidas en el artículo 2 de la Ley 2/2023 (como, por ejemplo, los relativos a acoso laboral o acoso sexual), todos ellos deberán converger bajo la supervisión del Responsable del Sistema Interno de Información, con el fin de ofrecer una “ventana única” de recepción y garantizar la aplicación uniforme de las garantías legales, en particular en materia de confidencialidad, seguridad, información al informante y cumplimiento de plazos.
- Protección contra represalias: Se deberá incluir en la normativa de la entidad un compromiso y una lista de garantías que aseguren la ausencia de represalias, incluyendo acciones como el despido, descenso de categoría, traslado o cualquier acto discriminatorio dirigidas contra la persona informante.
- El Sistema debe garantizar que se cumple con la obligación de informar al comunicante sobre:
 - Tratamiento de protección de datos y en su caso de la posibilidad de grabación de la conversación.
 - Notificación segura: Se debe ofrecer la posibilidad de que el informante pueda indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones oficiales
 - Canales externos: Se debe ofrecer información clara y accesible sobre la existencia de los canales externos de información ante las Autoridades Competentes
- **Externalización**: La gestión del SII podrá externalizarse en los términos legales previstos en la normativa, sin que ello altere que la responsabilidad última por su correcto funcionamiento y por el cumplimiento normativo recaiga íntegramente en la entidad obligada, debiendo el Responsable del Sistema cumplir siempre los requisitos de independencia exigidos.
- En el caso de **grupo de empresas**, la Ley 2/2023 configura la obligación de disponer de un Sistema Interno de Información como una obligación estrictamente individual, que debe analizarse de forma separada por cada sociedad integrante de un grupo empresarial, sin que la pertenencia a un grupo altere dicha exigencia. No obstante, la norma atribuye a la sociedad dominante funciones de dirección en materia de cumplimiento, permitiéndole aprobar una política general sobre el sistema interno de información y la defensa del informante, así como asegurar la aplicación de sus principios en el

¹ Asimismo, en el caso de que se reciban por error comunicaciones fuera de los canales establecidos, se debe remitir inmediatamente al Responsable del Sistema interno de información y mantener la confidencialidad.

conjunto del grupo. No obstante lo anterior, el documento publicado establece que cada entidad deberá nombrar individualmente al Responsable del Sistema interno de información (sin perjuicio de que dicho nombramiento pueda recaer en la misma persona para el caso de grupos de empresas).

- Dicha política general deberá respetar en todo caso la autonomía e independencia de cada entidad y contemplar las adaptaciones necesarias para garantizar el cumplimiento de la normativa aplicable en cada caso. En este contexto, es posible la existencia de un sistema interno de información único para el grupo —incluso cuando la sociedad matriz tenga su domicilio fuera de España— siempre que, respecto de cada entidad obligada, el sistema cumpla íntegramente las exigencias materiales, procedimentales y organizativas de la Ley 2/2023; de lo contrario, la entidad española no podrá considerarlo válido a efectos de cumplimiento legal.
- Responsable del Sistema interno de información (RSII): El documento de recomendaciones recuerda las funciones directivas requeridas en el caso del responsable del sector privado, así como la independencia en su actuación respecto al órgano de gobierno. En el caso del sector público, se señala que el RSII *“debería ser designado entre empleados públicos”*.
- Para el caso de designación de un RSII colegiado del sector privado, se recomienda que dicho órgano no supere los 5 miembros y establece que al menos la persona en quien se deleguen las funciones de gestión debería cumplir con los requisitos de la normativa. Asimismo, no se requiere que todos los miembros del órgano formen parte de la organización.
- En el caso del sector público la Autoridad sí que considera que todos los miembros del órgano colegiado deberían reunir los requisitos de la normativa y podrá dispensarse la condición del empleado público en uno de los miembros *“cuando resulte imprescindible recurrir a apoyo externo”*.
- Formación: Se deberá proporcionar formación e información suficiente a las personas trabajadoras sobre la existencia del canal y su correcto uso.

Esta circular tiene por objeto facilitar la identificación de los criterios interpretativos más relevantes fijados por la AIPI, sin sustituir ni reproducir el contenido íntegro de la Ley 2/2023 ni de su normativa de desarrollo.

Departamento de Nuevas Tecnologías y Cumplimiento Normativo de ARPA Abogados Consultores

Checklist básico - Recomendación 1/2026 (AIPI)

Diseño e implementación de un Sistema Interno de Información (SII)

Fuente: Sección III ("Lista de verificación básica") de la Recomendación 1/2026 de la Autoridad Independiente de Protección del Informante (AIPI).

- 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.