Afi Research

Nota sobre Regulatorio Financiero nº 3

Enero 2026

Recomendación 1/2026 de la Autoridad Independiente de Protección del Informante (AIPI). Implicaciones para el Consejo de Administración – Sector Privado

1. Objeto de la nota

Informar sobre el **alcance, relevancia e implicaciones prácticas** de la Recomendación 1/2026 de la Autoridad Independiente de Protección del Informante (AIPI), relativa al diseño e implementación del Sistema Interno de Información (SII), así como sobre las **decisiones estratégicas** que corresponde adoptar al órgano de administración para asegurar el cumplimiento de la Ley 2/2023 y mitigar riesgos regulatorios y reputacionales.

2. Relevancia estratégica de la Recomendación 1/2026

Aunque la Recomendación 1/2026 **no tiene carácter normativo**, constituye el **marco interpretativo de referencia** que previsiblemente aplicará la AIPI en sus funciones de supervisión y potestad sancionadora.

En la práctica:

- Eleva el estándar exigible a las empresas obligadas.
- Refuerza la responsabilidad del órgano de administración en la implantación y supervisión del SII.
- Incrementa el riesgo de cuestionamiento de sistemas meramente formales o deficientemente implantados.

La AIPI concibe el SII como una **infraestructura esencial de integridad y cumplimiento**, y no como un simple canal de denuncias.

3. Entidades del sector privado obligadas

Están obligadas a disponer de un Sistema Interno de Información conforme a la Ley 2/2023 y a los criterios de la Recomendación aquellas entidades del sector privado que:

- Desarrollen actividad en España mediante presencia organizada o establecimiento, sucursales o agentes, o incluso mediante prestación de servicios sin establecimiento permanente (con independencia del domicilio social).

- Cuenten con **50 o más personas trabajadoras**[1] **con independencia de la** modalidad contractual (contratos indefinidos, fijos discontinuos, contratos de duración determinada, contratos de puesta a disposición (ETT)).

  Además:

  - 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.

- Operen en sectores regulados por normativa de la Unión Europea (servicios financieros, prevención del blanqueo de capitales, transporte, medio ambiente), con independencia del número de trabajadores.

El cómputo de plantilla es amplio y debe revisarse periódicamente, incluyendo contratos temporales recientes y cualquier modalidad contractual.

4. Responsabilidad del Consejo de Administración

La Recomendación refuerza el papel del Consejo como **responsable último del Sistema Interno de Información**, atribuyéndole, de forma directa o indirecta, las siguientes funciones clave:

- **Aprobación formal** del Sistema Interno de Información.
- **Aprobación de la Política del SII** y del Procedimiento de gestión de informaciones.
- **Designación y, en su caso, cese del Responsable del Sistema Interno de Información (RSII)**.
- Garantía de que el RSII dispone de **independencia funcional y medios suficientes**.
- Supervisión del adecuado funcionamiento del sistema como parte del modelo de compliance y control interno.

La falta de implicación efectiva del Consejo incrementa el riesgo de responsabilidad corporativa.

[1] 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.

5. Características exigibles al Sistema Interno de Información

Desde la perspectiva del sector privado, el SII debe cumplir, como mínimo, los siguientes criterios:

a) Enfoque integral y preventivo

El sistema debe permitir a la empresa detectar, gestionar y corregir internamente posibles irregularidades antes de que se activen canales externos o procedimientos sancionadores.

b) Acceso amplio

El SII no se limita a empleados: debe estar disponible también para autónomos y profesionales independientes que trabajan para la empresa, proveedores, contratistas, extrabajadores y candidatos en procesos de selección.

c) Confidencialidad y seguridad reforzadas

Es imprescindible garantizar:

- Protección absoluta de la identidad del informante.
- Plataformas seguras, cifradas de extremo a extremo y con accesos restringidos.
- Trazabilidad controlada de las actuaciones.
- La confidencialidad se extiende 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.

d) Doble vía de comunicación

El sistema debe permitir comunicaciones:

- **Escritas**: mediante formularios electrónicos seguros, correo postal o correo electrónico.
- **Verbales**: mediante línea telefónica, mensajes de voz y, a solicitud del informante, reunión presencial con el Responsable del Sistema Interno de Información en un plazo máximo de siete días.

e) Gestión centralizada

En caso de existir varios canales sectoriales (por ejemplo, acoso laboral), estos deben integrarse bajo una **gestión unificada** y un único 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.

6. Política y procedimiento: documentos clave

La Recomendación exige la existencia de dos documentos formales, cuya aprobación corresponde al órgano de administración:

1. **Política del Sistema Interno de Información**, que debe definir:

   - Principios generales del sistema.
   - Garantías de confidencialidad, independencia y protección frente a represalias.
   - Derechos y deberes de informantes, personas afectadas y personas que gestionan la información.

   La política deberá ser de fácil acceso y adecuadamente difundida, de forma que todas las personas con una relación laboral o profesional con la entidad puedan conocerla.

2. **Procedimiento de gestión de informaciones**, escrito y formal que debe regular cada fase:

   - Acuse de recibo en un máximo de 7 días.
   - Resolución o respuesta en un máximo de 3 meses (ampliable en casos complejos).
   - Separación de funciones, la trazabilidad de las actuaciones y una gestión diligente e imparcial, y evitar retrasos, interferencias o usos indebidos del sistema.
   - Remisión inmediata a Fiscalía cuando existan indicios de delito.

Estos documentos son **elementos críticos en una eventual inspección o procedimiento sancionador**.

7. Responsable del Sistema Interno de Información (RSII)

El RSII es la figura operativa central del sistema (la designación de un Responsable del Sistema Interno de Información (RSII) es obligatoria) y debe:

- Actuar con **plena independencia** del equipo directivo y del propio Consejo.
- No recibir instrucciones sobre la gestión concreta de las informaciones.
- Disponer de recursos suficientes.

Puede ser:

- Una persona física (directivo o responsable de cumplimiento).
- Un órgano colegiado reducido, con perfiles complementarios. 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.

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.

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.

El nombramiento y cese deben notificarse a la autoridad competente dentro de los plazos legales.

8. Grupos empresariales

La Recomendación aclara que:

- La obligación de disponer de un SII es **individual por sociedad**, incluso dentro de un grupo.
- En los grupos de empresas, la sociedad dominante asume una función de dirección en materia de cumplimiento, consistente en aprobar una política general del sistema y asegurar su aplicación en el grupo, respetando siempre la autonomía de cada sociedad y las adaptaciones necesarias para cumplir la normativa aplicable.
- Puede existir un sistema y un responsable comunes (pero en el entendimiento de que la existencia de un sistema único no transforma al grupo en un único sujeto obligado), siempre que:

    - Cada sociedad se adhiera voluntariamente.
    - El sistema cumpla íntegramente la Ley 2/2023 respecto de cada entidad.
    - Cada sociedad designe formalmente al RSII.

Este punto es especialmente relevante en estructuras societarias complejas.

9. Riesgos y oportunidades para la compañía

Riesgos de incumplimiento

- Sanciones administrativas.
- Reputacionales.
- Pérdida de credibilidad del sistema de compliance.
- Activación directa de canales externos por falta de confianza interna.

Oportunidades

- Refuerzo del gobierno corporativo.
- Mejora de la cultura ética y de cumplimiento.
- Detección temprana de riesgos legales y operativos.
- Alineamiento con estándares europeos de integridad.

10. Próximos pasos recomendados al Consejo

Se recomienda al Consejo de Administración:

1. Verificar si el SII actual se ajusta a los criterios de la Recomendación 1/2026.
2. Revisar y, en su caso, actualizar la Política y el Procedimiento del SII.
3. Confirmar la idoneidad, independencia y medios del RSII.
4. Solicitar un informe periódico sobre el funcionamiento del sistema.
5. Integrar el SII en la agenda regular de supervisión del modelo de compliance.

Patricia Muñoz González-Úbeda
Socia directora de Regulatorio Financiero e Interlocución con Supervisores de Afi