17/07/2026

La Autoridad Independiente de Protección del Informante fija un nuevo estándar para los canales internos de información en la Administración del Estado

por Iván Martínez, CEO de Intedya

La Autoridad Independiente de Protección del Informante (AIPI) ha publicado la Recomendación 3/2026, de 7 de julio, relativa al diseño e implementación de los Sistemas Internos de Información en la Administración General del Estado y en sus entidades instrumentales de Derecho público. El documento desarrolla la aplicación práctica de la Ley 2/2023 en ministerios, organismos autónomos, agencias estatales, entidades públicas empresariales, consorcios y otras entidades públicas vinculadas o dependientes de la Administración estatal. Aunque la Recomendación no tiene carácter normativo ni crea obligaciones adicionales, la propia AIPI advierte de que podrá valorar su grado de seguimiento cuando supervise el funcionamiento de estos sistemas, por lo que sus criterios están llamados a convertirse en una referencia relevante de cumplimiento.

El canal no es suficiente: debe existir un sistema completo

Uno de los mensajes centrales del documento es que cumplir la Ley 2/2023 no consiste únicamente en habilitar un formulario o un buzón de denuncias. El Sistema Interno de Información debe integrar el canal de recepción, el Responsable del Sistema Interno de Información —RSII— y un procedimiento formal para admitir, investigar, resolver y archivar las comunicaciones.

La AIPI concibe este sistema como una pieza de la integridad institucional, capaz de detectar irregularidades y corregirlas antes de que produzcan consecuencias jurídicas, económicas o reputacionales más graves. Esta visión obliga a analizar no solo la existencia del canal, sino también quién controla la investigación, cómo se protege la información y qué garantías reales recibe la persona informante.

Cada entidad debe disponer de su propio sistema

La Recomendación señala que cada entidad obligada debe contar con un sistema propio y funcionalmente independiente. La pertenencia a un mismo ministerio no permite que organismos autónomos, agencias o entidades dependientes queden automáticamente cubiertos por el canal ministerial. La compartición de medios será posible en los supuestos legalmente previstos, especialmente en entidades de menor tamaño, pero deberá existir un acuerdo formal, una identificación clara de la entidad titular y garantías individualizadas para las personas informantes. Por tanto, no se considera adecuado que un ministerio centralice sin más las comunicaciones de todos sus organismos dependientes.

El ámbito de protección tampoco se limita al personal funcionario. El canal debe poder ser utilizado por personal laboral, eventual y directivo, altos cargos, becarios, personas en prácticas, contratistas, proveedores, licitadores, antiguos empleados, aspirantes a procesos selectivos y miembros de órganos de gobierno o supervisión.

La independencia del responsable, principal punto crítico

La Recomendación identifica la independencia del RSII como uno de los elementos más sensibles del sistema. En organizaciones fuertemente jerarquizadas, la autonomía formal puede resultar insuficiente si la persona responsable depende orgánica o funcionalmente de quienes podrían verse afectados por una investigación. Para ministerios y organismos de gran tamaño o con un

riesgo elevado de conflicto, la AIPI recomienda preferentemente un órgano colegiado de entre tres y cinco miembros, con perfiles técnicos en Derecho administrativo sancionador, control interno, contratación pública, auditoría, intervención o cumplimiento normativo.

La colegialidad permite distribuir responsabilidades, reforzar la continuidad del sistema y reducir el riesgo de interferencias. También se aconseja que los miembros dispongan de un mandato estable, que existan suplentes y que se evite la designación de personas con vínculos políticos recientes, relaciones familiares relevantes o situaciones que puedan comprometer su imparcialidad.

La AIPI cuestiona el papel de las Inspecciones Generales de Servicios

Uno de los apartados de mayor impacto es el dedicado a las Inspecciones Generales de Servicios. Aunque estas unidades cuentan con experiencia investigadora y conocimiento de la organización, la AIPI identifica riesgos derivados de su dependencia de la Subsecretaría, de su obligación de reportar a la jerarquía y de sus competencias ordinarias sobre recursos humanos, contratación, subvenciones y gestión interna.

La Recomendación no invalida las designaciones existentes ni tiene efectos retroactivos, pero invita a revisar estos modelos cuando se produzca la renovación del responsable. Cuando no exista otra alternativa, se aconseja que la persona designada no sea la titular de la jefatura de la Inspección y que actúe de forma separada respecto de sus funciones ordinarias.

Este criterio puede obligar a numerosos organismos a replantear quién gestiona actualmente sus canales internos.

Cuatro modelos de organización

La AIPI distingue entre la responsabilidad material del sistema y la gestión técnica de la plataforma. A partir de esta separación plantea cuatro modelos: sistema propio con gestión interna, sistema propio con plataforma externa, sistema compartido con gestión interna y sistema compartido con plataforma externa.

Para ministerios y grandes organismos se considera preferente mantener un RSII propio y recurrir a una plataforma tecnológica especializada, mientras que para entidades pequeñas puede resultar más adecuado compartir el sistema y externalizar conjuntamente la infraestructura.

En todo caso, la externalización debe limitarse al soporte técnico. La admisión, investigación y resolución de los expedientes seguirá correspondiendo al RSII, sin que estas decisiones puedan trasladarse al proveedor.

Estanqueidad tecnológica y separación de los sistemas corporativos

La Recomendación establece una interpretación exigente de la confidencialidad técnica. La información del canal no debería circular por el correo corporativo, Microsoft Teams, gestores documentales administrativos, SharePoint, carpetas de red o dispositivos personales no autorizados.

La plataforma debería estar separada de los sistemas ordinarios de la entidad y disponer de autenticación multifactor, cifrado, registros inmutables de acceso y capacidad para recibir comunicaciones anónimas sin almacenar metadatos identificativos como direcciones IP o huellas del navegador.

Este planteamiento afecta directamente a muchos sistemas implantados mediante herramientas corporativas convencionales, ya que la AIPI considera que la confidencialidad debe preservarse durante todas las fases del expediente y no solo en el momento inicial de la comunicación.

También recomienda realizar una Evaluación de Impacto en Protección de Datos antes de la puesta en funcionamiento del canal, especialmente para analizar los riesgos de reidentificación, el tratamiento de datos de terceros y los plazos de conservación. El Delegado de Protección de Datos podrá asesorar y supervisar, pero no debería asumir funciones ejecutivas de admisión, investigación o decisión.

Un procedimiento más detallado y trazable

La Ley establece un plazo de siete días naturales para el acuse de recibo y un máximo de tres meses para responder, ampliable a seis en casos complejos. La AIPI desarrolla estas previsiones mediante un procedimiento orientativo de once fases que incluye recepción, evaluación preliminar, decisión de admisión, plan de investigación, audiencia de la persona afectada, seguimiento periódico, resolución y archivo seguro.

Entre las principales novedades se propone realizar la evaluación preliminar en quince días hábiles, aprobar el plan de investigación en los diez días posteriores a la admisión e informar al denunciante sobre el estado del expediente cada treinta días, siempre que ello no comprometa la investigación.

Cuando existan indicios de delito, el RSII deberá remitir directamente la información al Ministerio Fiscal, sin solicitar autorización ni informar previamente a la jerarquía ministerial. El mismo criterio se aplicará en relación con la Fiscalía Europea o con otras autoridades competentes cuando los hechos afecten a los intereses financieros de la Unión Europea o constituyan infracciones administrativas.

Protección frente a represalias en el empleo público

La Recomendación dedica especial atención a las represalias indirectas, que en la Administración no suelen adoptar la forma de un despido, sino de decisiones relacionadas con la carrera, la productividad, las funciones o la movilidad.

La AIPI menciona como posibles señales de represalia los ceses en puestos de libre designación, evaluaciones negativas no justificadas, denegaciones de permisos, apertura de expedientes disciplinarios, traslados forzosos, reducción de productividad, asignación de tareas de menor relevancia, exclusión de proyectos o retrasos en el reconocimiento de derechos económicos.

En estos casos resulta especialmente importante la inversión de la carga de la prueba prevista en la Ley 2/2023. Cuando una persona acredite que realizó una comunicación protegida y posteriormente sufrió un perjuicio, corresponderá a la Administración demostrar que la medida respondía a razones objetivas y ajenas a la denuncia.

Ante una posible represalia, el RSII debería reunirse en un plazo máximo de cuarenta y ocho horas, valorar la suspensión cautelar de la medida y abrir un expediente interno de salvaguarda que permita documentar la evolución del caso y generar trazabilidad probatoria.

Protocolos reforzados para altos cargos

La Recomendación también aborda las comunicaciones que afectan a directores generales, subsecretarios, secretarios de Estado o ministros. En estos casos se exige una especial separación respecto de la jerarquía y se recomienda evitar que la existencia del expediente sea comunicada antes de tiempo si ello puede comprometer la investigación.

Cuando la información afecte a los niveles más altos, podrá recurrirse a instructores externos, funcionarios ajenos al departamento, miembros ad hoc o mecanismos reforzados de abstención y recusación. Si existen indicios de delito, la remisión a la Fiscalía deberá realizarse directamente.

Este punto resulta especialmente relevante porque la eficacia del sistema se mide, en gran parte, por su capacidad para investigar con independencia incluso cuando los hechos afectan a la cúpula de la organización.

Formación, transparencia y evaluación periódica

La AIPI recomienda que el acceso al canal sea visible desde la página principal y esté claramente separado de los buzones de quejas y sugerencias. También propone publicar información sobre la composición del RSII, los derechos del informante, estadísticas agregadas, tiempos medios de tramitación y una memoria anual de actividad.

En materia de formación, plantea un mínimo de cuatro horas para el conjunto del personal y veinte horas anuales para los

miembros del RSII, con contenidos sobre técnicas de entrevista, análisis documental, prueba indiciaria, protección de datos y prevención de represalias.

Además, el sistema debería revisarse periódicamente para identificar fallos, patrones de riesgo y oportunidades de mejora, de modo que las comunicaciones no se limiten a resolver casos individuales, sino que contribuyan al aprendizaje institucional.

Una referencia que obligará a revisar muchos sistemas existentes

La Recomendación 3/2026 no modifica la Ley 2/2023, pero eleva considerablemente el nivel de exigencia esperado. No seguir todos sus criterios no implica automáticamente un incumplimiento, aunque cualquier modelo alternativo deberá ser capaz de demostrar que ofrece garantías equivalentes.

Su aplicación obligará previsiblemente a revisar designaciones, procedimientos, plataformas tecnológicas, contratos con proveedores, medidas de protección de datos y protocolos frente a represalias.

La principal conclusión es clara: la Administración ya no podrá considerar suficiente la existencia formal de un canal. La eficacia del sistema dependerá de su independencia real, de su estanqueidad tecnológica, de la calidad de las investigaciones y de su capacidad para proteger al informante incluso cuando la comunicación afecte a los niveles más altos de la organización.