



Recomendación

**2/2026 de la Autoridad Independiente
de Protección del Informante
para el diseño e implementación
de un Sistema Interno de Información
en la Administración Local (v3)**

Madrid, julio de 2026

CONTROL DE VERSIONES	
Nº de versión	Fecha
Versión 1	13 de enero de 2026
Versión 2	29 de enero de 2026
Versión 3	13 de julio de 2026



Recomendación 2/2026 de la Autoridad Independiente de Protección del Informante para el diseño e implementación de un Sistema Interno de Información en la Administración Local. Versión 3.

© Autoridad Independiente de Protección del Informante, 2026.

<https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.es>

Esta obra está bajo una licencia Creative Commons Atribución-NoComercial 4.0 Internacional (CC BY-NC SA 4.0). Esta licencia permite a los reutilizadores del material distribuir, remezclar, adaptar y desarrollar el material en cualquier medio o formato, exclusivamente con fines no comerciales, y siempre que se atribuya la autoría al creador. Si remezcla, adapta o desarrolla el material, debe licenciar el material modificado bajo términos idénticos.

<https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.es>



Reconocimiento - No Comercial - Compartir Igual (BY-NC-SA)

Índice

INTRODUCCIÓN	4
I. OBJETIVO Y DESTINATARIOS	5
II. ANÁLISIS DEL MARCO NORMATIVO RELATIVO AL SISTEMA INTERNO DE INFORMACIÓN EN LA LEY 2/2023 (LPI).....	6
II.1.- Configuración del Sistema Interno de Información (SII)	6
II.2. El Responsable del Sistema Interno de Información (RSII)	12
II.3. Características mínimas de diseño del canal interno de información (CII)	14
II.4. Procedimiento de gestión de información: obligaciones	18
III. EVALUACIÓN PERIÓDICA Y MEJORA CONSTANTE	20
IV. LISTA DE VERIFICACIÓN BÁSICA PARA EL DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA INTERNO DE INFORMACIÓN EN LA ADMINISTRACIÓN LOCAL.....	21

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, 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”*.

Esta Autoridad, desde su puesta en funcionamiento en septiembre de 2025, ha recibido numerosas consultas y ha constatado la existencia de dudas interpretativas recurrentes en el ámbito de la administración local. En el marco de su actividad institucional, y tras la reunión mantenida con la Federación Española de Municipios y Provincias (FEMP), esta Presidencia considera necesario establecer pautas de funcionamiento sobre el cumplimiento de las obligaciones de la Ley respecto a los sistemas internos de información.

A resultas de esta reunión, esta Presidencia elabora el siguiente documento que se configura como una orientación dirigida a los Ayuntamientos y a las entidades que integran la Administración Local, destinada a facilitar el diseño, la correcta implantación y funcionamiento del Sistema Interno de Información conforme a la Ley 2/2023, de 20 de febrero, respetando en todo caso la autonomía organizativa local y sin que tenga carácter normativo ni vinculante.

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

Recomendación AIPI 2/2026 (v3) para el diseño e implementación de un Sistema Interno de Información en la Administración Local

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, entre otras, a las Administraciones públicas, ya sean territoriales o institucionales.

En concreto, el artículo 13.1 de la Ley dispone que todas las entidades que integran el sector público estarán obligadas a disponer de un Sistema Interno de Información, considerando a los efectos de esta ley comprendidos en el 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.***

*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, aprobado por Real Decreto Legislativo 4/2015, de 23 de octubre.*

El objeto específico de esta Recomendación es orientar el cumplimiento de las obligaciones contenidas en la Ley 2/2023, de 20 de febrero, a las entidades que integran **la Administración Local**, todo ello sin perjuicio de las competencias que puedan tener, en su caso, las autoridades autonómicas de protección del informante y del debido respeto a la potestad autoorganizativa de la Administración Local.

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 (en este caso, por la Administración Local).

II.1.1. Sujetos obligados (art. 13)

Conforme al artículo 13 de la Ley, la obligación de disponer de un Sistema Interno de Información abarca a **todas las entidades del sector público local**, en concreto:

1. Las entidades que integran la Administración local (Municipios, Provincias, Islas, Comarcas, Áreas Metropolitanas, Mancomunidades, etc.)
2. Los organismos y entidades públicas vinculadas o dependientes de alguna Administración pública local.

3. Las sociedades mercantiles y fundaciones del sector público local, entendiendo por tales aquellas en cuyo capital social o patrimonio la participación, directa o indirecta, de las entidades locales sea mayoritaria o en las que se ejerza control de gestión.

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 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: Es recomendable que el SII sea 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 permitiendo presentar comunicaciones al menos, a:

- Personal al servicio de la entidad local, con independencia de la naturaleza de su vínculo (funcionarios, personal laboral, interinos, personal eventual).
- Becarios, personal en prácticas o personas en formación, aunque no exista una relación laboral formal.
- Autónomos y profesionales independientes que presten servicios a la entidad local (por ejemplo, arquitectos, abogados, técnicos externos, formadores, etc.).

- Personas que trabajen para empresas proveedoras, contratistas o concesionarias que mantengan una relación contractual con la entidad local (limpieza, mantenimiento, obras, servicios sociales, suministro de bienes, etc.).

- Personas cuya relación profesional ya haya finalizado, tales como exempleados municipales, antiguos contratistas o proveedores.

- Personas cuya relación profesional aún no haya comenzado, como aspirantes en procesos selectivos, personas participantes en bolsas de empleo o candidatas a futuras colaboraciones profesionales.

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 en las entidades locales es una garantía esencial tanto para la protección efectiva de las personas informantes como para el correcto funcionamiento y la eficacia del propio sistema. Es conveniente que esta confidencialidad se incorpore desde el inicio en el diseño organizativo y funcional del SII, teniendo en cuenta la especial cercanía personal y profesional existente en muchas organizaciones municipales.

A tal efecto, se recomienda que el sistema se gestione a través de canales seguros, cifrados de extremo a extremo, que garanticen la confidencialidad de la identidad del informante y de cualquier tercero mencionado, con accesos estrictamente limitados al personal expresamente autorizado, evitando la identificación directa o indirecta de las personas implicadas. La plataforma segura debería disponer de un registro de accesos y actuaciones (trazabilidad controlada).

Es conveniente que la confidencialidad se extienda no solo a la identidad, sino también al contenido de las comunicaciones, a las actuaciones desarrolladas durante su tramitación y a cualquier dato que permita inferirla, debiendo adoptarse medidas técnicas y organizativas adecuadas para proteger los datos personales, impedir accesos no autorizados y prevenir usos indebidos del sistema o posibles represalias.

- 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.

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.”

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 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 solo 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”.*

Implicación práctica: El procedimiento de gestión del SII en las entidades locales debería configurarse de manera ágil, clara y eficaz, garantizando tiempos de respuesta razonables y proporcionados a su estructura organizativa y a los medios disponibles. En particular, es clave asegurar la ausencia de represalias frente a las personas informantes y una actuación objetiva e imparcial en la tramitación de las comunicaciones.

También resulta muy conveniente que la entidad local transmita una comunicación institucional clara e inequívoca, que refuerce la confianza en que las informaciones recibidas serán tratadas con seriedad, confidencialidad y neutralidad, incluso en organizaciones municipales de pequeño tamaño. Todo ello favorece la detección temprana de posibles irregularidades y su corrección dentro del propio ámbito local, promoviendo una cultura de integridad y autocorrección en la gestión de los asuntos públicos.

- **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: El SII de la entidad local debería configurarse como un sistema propio y claramente identificable, que no pueda confundirse con los sistemas de otras administraciones, entidades dependientes, organismos supramunicipales o entes con los que el ayuntamiento mantenga relaciones funcionales, institucionales o contractuales. Esta exigencia resulta especialmente relevante en el ámbito local, donde es habitual la colaboración con diputaciones, mancomunidades, consorcios u otras entidades públicas.

A tal efecto, el canal o portal de acceso al sistema posibilitaría la identificación de forma clara e inequívoca la entidad local titular del SII y delimitar su ámbito de aplicación, de modo que la persona informante conozca con certeza ante qué entidad está comunicando la información y bajo qué régimen de garantías será tratada. Esta recomendación cobra especial importancia en los supuestos que se haga uso de la posibilidad prevista en el artículo 14 de la Ley y se comparta el SII.

- **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: De conformidad con lo anterior, cada entidad local debería aprobar una política o estrategia formal en materia de SII y protección de las personas informantes, en la que se recojan de forma clara los principios generales de funcionamiento del sistema, las garantías de confidencialidad, independencia y ausencia de represalias, así como los derechos y deberes de las personas informantes, de las afectadas por las comunicaciones y de quienes gestionan el sistema.

Es recomendable que dicha política sea accesible y difundida de manera adecuada dentro de la organización municipal (intranet, tablones, web pública), de modo que todas las personas que mantengan una relación laboral o profesional con la entidad conozcan la existencia del SII, los canales disponibles y el alcance de la protección ofrecida, favoreciendo que las posibles irregularidades se comuniquen, con carácter preferente, en el ámbito interno de la propia entidad local.

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

Implicación práctica: Debería 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). Este protocolo garantizaría 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 y segura, evitando retrasos injustificados, interferencias o cualquier uso indebido del sistema, con especial atención a la realidad organizativa de las entidades locales y, en particular, en los municipios de menor tamaño.

- 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 debería 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)

- **Externalización:** 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.

Si se hace uso de esta posibilidad, la gestión se limitará únicamente al procedimiento para la recepción de informaciones sobre infracciones y tendrá carácter exclusivamente instrumental.

- **Compartición:** 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.

Esta posibilidad resulta especialmente útil para poder hacer frente a las exigencias que impone la Ley en esta materia, en la medida que no sólo permite compartir el SII, sino también los recursos para la gestión, lo que abre la vía a compartir costes que de otro modo pueden resultar excesivamente gravosos de implementar individualmente.

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 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, sería recomendable excluir 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.

- **Órgano colegiado:** La designación de un órgano colegiado como RSII puede resultar especialmente adecuada en determinadas entidades locales, al reforzar la confianza en el sistema, permitir el reparto de responsabilidades y reducir el riesgo de interferencias o instrumentalización, especialmente en contextos de proximidad organizativa.

Para garantizar su operatividad, el órgano no debería superar los cinco miembros y delegar en uno de ellos las funciones de gestión y tramitación de los expedientes de investigación. No será necesario que todos los integrantes pertenezcan a la entidad local, si bien el órgano deberá contar, al menos, con un miembro interno. En todo caso, el órgano colegiado asumirá la responsabilidad del Sistema Interno de Información de la entidad, con independencia del origen de sus miembros.

Cuando el Sistema Interno de Información sea gestionado por un órgano colegiado, lo ideal es que la designación y el perfil de sus miembros se ajuste a los criterios establecidos para los casos en que el RSII cuando sea una persona física. En particular, sería deseable que los miembros fueran preferentemente empleados públicos con las garantías establecidas por la Ley. La posibilidad de que los miembros del órgano fuesen directivos públicos cargos electos y responsables políticos, o incluso miembros externos con perfiles técnicos o jurídicos debería utilizarse con precaución y en estos casos resultaría necesario reforzar las garantías y establecer:

- Reglas estrictas de confidencialidad: compromisos individuales firmados, reglas de acceso restringido a la información, etc.).
 - Reglas para abordar conflictos de intereses, abstenciones y sustituciones (estar previsto cuándo un miembro se abstiene, quién lo sustituye, cómo se documenta, etc.).
- **Compatibilidad de funciones:** Si ya existiera 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. En aquellas entidades con estructura que no justifique la dedicación exclusiva del RSII, sus funciones podrán compatibilizarse con otras, siempre que se garantice la ausencia de conflictos de interés y la total independencia en el ejercicio de su labor.

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 de la entidad obligada.

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. 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.

En el caso de que el nombramiento recaiga en un órgano colegiado, será necesario comunicar tanto el nombramiento, como el cese de todos los integrantes del órgano colegiado, identificando de forma concreta en cuál de ellos se ha delegado la gestión del sistema interno y la tramitación de expedientes de investigación.

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.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.

Sería aconsejable que las Entidades locales proporcionasen en su página web información adecuada de forma clara y fácilmente accesible, sobre el uso del canal, así como sobre los principios esenciales del procedimiento de gestión. Dicha información constaría en la página

de inicio, en una sección separada y fácilmente visible y diferenciada respecto del buzón de quejas y sugerencias.

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) , asegurando la unidad de gestión y procedimiento (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.3.2. 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.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 canal 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. Requisitos técnicos mínimos de la plataforma

Con arreglo a la Ley 2/2023, la Directiva (UE) 2019/1937, el Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo) y el RGPD, se recomienda que la plataforma del CII garantice de forma proporcionada a la dimensión, los medios y el nivel de riesgo de cada entidad, las siguientes características. No se trata de trasladar al canal interno las exigencias técnicas y organizativas propias del canal externo gestionado por la AIPI, que responden a su naturaleza y a su ámbito de actuación, sino de ofrecer un conjunto de criterios de referencia que cada entidad podrá modular en su implantación:

1. **Cifrado de extremo a extremo (E2E)** conforme al estándar TLS 1.3 o superior, tanto en las comunicaciones como en el almacenamiento de datos en reposo.
2. **Separación lógica y física de la base de datos del SII** respecto de los sistemas corporativos de la entidad (GEISER, SIR, correo corporativo, intranet).

Autenticación multifactor (MFA) para el acceso del RSII (persona física o integrantes del órgano colegiado).

Registro de auditoría inmutable (**audit log**) de cada acceso al sistema: quién accede, desde qué terminal, en qué fecha y hora y a qué expediente. Se recomienda que este registro resulte inaccesible para los administradores de sistemas de la entidad y quede reservado al RSII, sin perjuicio del acceso de la AIPI cuando lo precise en el ejercicio de sus funciones de supervisión.

3. **Capacidad para la recepción de comunicaciones anónimas** sin que la plataforma registre metadatos identificativos del informante (dirección IP, huella digital del navegador, cookies de sesión).

Acceso multicanal: formulario web seguro, línea telefónica dedicada o, en su defecto, un sistema de mensajería de voz integrado en la propia plataforma y correo electrónico cifrado específico, distintos en todo caso de los canales corporativos ordinarios de la entidad.

4. **Accesibilidad universal** conforme al estándar WCAG 2.1, nivel AA, y disponibilidad en las lenguas cooficiales cuando la entidad tenga competencias en territorios con lengua propia.

II.3.5. Conexión con el Libro-Registro (artículo 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	Es un requisito de transparencia del CII que el RSII debe garantizar en la documentación.

	(AAI) y, en su caso, ante las instituciones de la Unión Europea.	
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. <i>Excepción:</i> 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 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 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.4.3 Conexión funcional entre los diferentes elementos que integran el SII

El procedimiento (art. 9) es el vínculo operativo que une los principales elementos del Sistema Interno de Información:

- SII (art. 5) ↔ Procedimiento (art. 9): El Procedimiento es la materialización del principio del “debido proceso (art. 5.2.i)” y “efectividad (art. 5.2.e) del Sistema”.
- RSII (art. 8) ↔ Procedimiento (art. 9): El RSII es el gestor responsable que ejecuta todas las obligaciones temporales y procesales (art. 9.2.c, d, f, j).
- CII (art. 7) ↔ Procedimiento (art. 9): El Canal es la herramienta técnica que debe soportar los requisitos del procedimiento, como el acuse de recibo, la comunicación bidireccional y la admisión del anonimato.

III. EVALUACIÓN PERIÓDICA Y MEJORA CONSTANTE

La obligación de disponer de un Sistema Interno de Información no se limita a su mera implementación, ni a la gestión puntual de las informaciones que se reciban. Por el contrario, exige un compromiso y mantenimiento continuo por parte de la organización que incluye la realización de evaluaciones periódicas sobre su funcionamiento y eficacia.

Asimismo, resulta imprescindible prever y activar mecanismos de análisis y corrección que, a la vista de las denuncias o incidencias detectadas, permitan identificar las causas subyacentes y adoptar medidas adecuadas para evitar que dichos problemas se reproduzcan en el futuro, reforzando así la cultura de cumplimiento y mejora continua en las entidades locales.

En este contexto, se recomienda que el Sistema trascienda su función reactiva para convertirse en una fuente estratégica de aprendizaje institucional. No basta con resolver el caso concreto; es necesario nutrirse de la propia experiencia del canal ("aprender del sistema"). Esto implica establecer ciclos de retroalimentación que evalúen no solo el fondo de las denuncias, sino la calidad y accesibilidad del procedimiento en sí mismo.

Por tanto, es aconsejable que la organización analice periódicamente los patrones sistémicos detectados y solicitar la valoración de los usuarios del canal, siempre respetando la confidencialidad, para perfeccionar los protocolos. De este modo, el Sistema Interno de Información actúa como un termómetro en tiempo real de la ética organizativa, transformando cada comunicación en una oportunidad para recalibrar el mapa de riesgos y elevar los estándares de integridad corporativa.

IV. LISTA DE VERIFICACIÓN BÁSICA PARA EL DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA INTERNO DE INFORMACIÓN EN LA ADMINISTRACIÓN LOCAL

- ☐ Consulta previa a la representación sindical.
- ☐ Acuerdo del Órgano de Gobierno (Pleno/Junta) 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 empleado público sobre el uso del canal.



Autoridad Independiente
de Protección del Informante