OFICINA **ANDALUZA** ANTIFRAUDE

CANALES INTERNOS

Guía jurídica y técnica

ÍNDICE

INTRODUCCIÓN

El 13 de marzo de 2023 entró en vigor 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 supone la transposición al ordenamiento jurídico nacional de la Directiva 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019.

Dicha Ley establece el régimen jurídico de los sistemas internos de información que abarcan tanto el canal interno, entendido como buzón o cauce para la recepción de la información, como las políticas y procedimientos indispensables para una eficaz protección de las personas que deciden denunciar.

La presente guía, elaborada por la Oficina Andaluza contra el Fraude y la Corrupción, se dirige a dichas entidades y pretende facilitar el proceso de implantación de los sistemas internos de información y sus correspondientes canales internos de denuncia.

La guía se estructura en dos apartados, el primero recoge información jurídica relevante de la normativa europea, española y andaluza de aplicación en lo que respecta al diseño, procedimientos y gestión de los sistemas internos de información, mientras que el segundo apartado se centra en los requisitos y aspectos técnicos que debe reunir la implementación de un canal de denuncias a través de internet.

1. INFORMACIÓN JURÍDICA

1.1. CONCEPTOS

Existe una clara diferenciación entre un sistema interno de información, un canal interno y un canal externo de información.

Sistema Interno de Información (SII): Concepto más amplio que canal o buzón interno, que parte de la diversidad de organizaciones sujetas al cumplimiento de la Directiva 2019/1937, bien sean organizaciones públicas o privadas.

El SII, tal y como se representa en el esquema, abarca tanto el canal, entendido como buzón o cauce para recepción de la información, como la persona Responsable del Sistema, el procedimiento de gestión de información, la estrategia que enuncie los principios generales en materia de SII y defensa del informante, así como las garantías de protección.

Canal Interno de Información: Instrumento integrado dentro del SII de cada entidad que posibilite la presentación de una denuncia interna.

Canal Externo de Información: canal gestionado por autoridad pública independiente, ante el que se podrán denunciar infracciones, ya sea directamente, o con posterioridad a la previa formulación de información ante el canal interno correspondiente. En Andalucía corresponde a la Oficina Andaluza contra el Fraude y la Corrupción.

1.2. SISTEMA INTERNO DE INFORMACIÓN

Implantación: El órgano de administración u órgano de gobierno de cada entidad u organismo será el responsable de la implantación del SII, previa consulta con la representación legal de los trabajadores. Tendrá la condición de responsable del tratamiento de los datos personales de conformidad con la normativa sobre protección de datos personales.

Los requisitos que debe cumplir el SII son:

- Integrar los distintos canales internos de información que pudieran establecerse dentro de la entidad.
- Permitir la comunicación de información sobre infracciones incluidas en el ámbito de la Ley 2/2023.
- Garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la correspondiente entidad u organismo con el objetivo de que la primera en conocer la posible irregularidad sea la propia entidad u organismo.
- Ser independientes y aparecer diferenciados respecto de los sistemas internos de información de otras entidades u organismos.
- Contar con una persona Responsable del Sistema, designada por el órgano de administración u órgano de gobierno de cada entidad obligada, previa consulta con la representación legal de las personas trabajadoras.
- Contar con una política o estrategia que enuncie los principios generales en materia de Sistemas interno de información y defensa del informante y que sea debidamente publicitada en el seno de la entidad u organismo.
- Contar con un procedimiento de gestión de las informaciones recibidas.
- Establecer las garantías para la protección de las personas informantes en el ámbito de la propia entidad u organismo.

1.3. CANAL INTERNO DE INFORMACIÓN

Integrado en el SII se creará el canal interno de información que posibilite la presentación de denuncias internas.

Denuncia interna: comunicación verbal o por escrito de información sobre infracciones dentro de una entidad jurídica de los sectores privado o público.

1.3.1. Prescripciones obligatorias

El canal interno cumplirá con las siguientes prescripciones obligatorias:

Confidencialidad y anonimato:

- Estarán diseñados, establecidos y gestionados de una forma segura, que garantice que la confidencialidad de la identidad del denunciante y de cualquier tercero mencionado en la denuncia esté protegida, e impida el acceso a ella al personal no autorizado.

  Esto se aplicará a cualquier dato del que se pueda deducir directa o indirectamente la identidad del informante. Su identidad únicamente podrá ser transmitida al Ministerio Fiscal o a la autoridad administrativa o judicial competente en el marco de un procedimiento disciplinario, penal o sancionador, cuando así lo establezcan las leyes.

- En el caso de denuncias anónimas debe garantizarse el anonimato del informante.

Vías de denuncia:

- Permitirán denunciar por escrito o verbalmente, o de ambos modos.
  - La denuncia escrita será posible por correo postal o por cualquier medio electrónico habilitado al efecto.
  - La denuncia verbal será posible por vía telefónica o a través de otros sistemas de mensajería de voz.
- La denuncia también será posible, previa solicitud del denunciante, por medio de una reunión presencial dentro de un plazo razonable (plazo máximo de 7 días)

Tramitación:

- Plazo de acuse de recibo: En un plazo no superior a siete días naturales desde la recepción de la denuncia, se debe emitir acuse de recibo a la persona denunciante.
- Plazo de respuesta: En un plazo no superior a tres meses se debe dar respuesta a la denuncia. El plazo contará desde el acuse de recibo o a partir del vencimiento del plazo de siete días después de interponerse la denuncia, en el caso de que no se hubiese emitido acuse de recibo. En casos de especial complejidad, podrá ampliarse un máximo de 3 meses adicionales.

Seguimiento:

- Debe designarse una persona o departamento imparcial que sea competente para realizar el seguimiento las denuncias, que podrá ser la misma persona o departamento que recibe las denuncias y que mantendrá la comunicación con el denunciante y, en caso necesario, solicitará a este información adicional y le dará respuesta.
- Debe efectuarse un seguimiento diligente por parte de la persona o el departamento designados, incluso cuando sean denuncias anónimas.

Información obligatoria:

- Deben contener información clara y fácilmente accesible sobre los procedimientos de denuncia externa ante las autoridades competentes, - en el caso de Andalucía ante la Oficina Andaluza contra el Fraude y la Corrupción- y en su caso ante las instituciones y organismos de la UE.

1.3.2. Gestión

Los canales de denuncia podrán gestionarse internamente por una persona o departamento designados al efecto o podrán ser proporcionados externamente por un tercero.

Gestión por tercero externo:

- A estos efectos, se considerará gestión del sistema, la recepción de información.
- Ha de ofrecer garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto.
- Pueden ser proveedores de plataformas de denuncia externa, asesores externos, auditores, representantes sindicales o representantes de los trabajadores.
- En el caso de Administraciones, la gestión por tercero externo solo podrá acordarse cuando se acredite insuficiencia de medios propios, y comprenderá únicamente el procedimiento para la recepción de las informaciones sobre infracciones y, en todo caso, tendrá carácter exclusivamente instrumental.

Medios compartidos:

Las entidades jurídicas del sector privado que tengan entre 50 y 249 trabajadores podrán compartir recursos para la recepción de denuncias y toda investigación que deba llevarse a cabo, sin perjuicio de las obligaciones impuestas a dichas entidades de mantener la confidencialidad, de dar respuesta a la persona denunciante y de tratar la infracción denunciada.

Los municipios de menos de 10.000 habitantes, entre sí o con cualesquiera otras Administraciones públicas que se ubiquen dentro del territorio de la comunidad autónoma, podrán compartir el SII y los recursos destinados a las investigaciones y las tramitaciones.

Las entidades pertenecientes al sector público con personalidad jurídica propia vinculadas o dependientes de órganos de las Administraciones territoriales, y que cuenten con menos de cincuenta trabajadores, podrán compartir con la Administración de adscripción el SII y los recursos destinados a las investigaciones y las tramitaciones.

En todo caso, deberá garantizarse que los sistemas resulten independientes entre sí y los canales aparezcan diferenciados respecto del resto de entidades u organismos, de modo que no se genere confusión a los ciudadanos.

1.3.3. Entidades obligadas

Sector Público

- Todas las entidades jurídicas del sector público deberán tener canal interno de denuncias, incluidas las entidades dependientes y sujetas al control de las mismas.
- Los organismos constitucionales y de relevancia constitucional e instituciones autonómicas análogas.

  Los SII y sus correspondientes canales que ya tuvieran habilitados las entidades u organismos obligados podrán servir para dar cumplimiento a las previsiones que establece la normativa siempre y cuando se ajusten a los requisitos establecidos en la misma (Disp. Transitoria 1ª Ley 2/2023).

Sector privado

- Todas las personas físicas o jurídicas del sector privado que tengan 50 o más trabajadores deberán tener un SII.
- Las entidades jurídicas del sector privado que entren en el ámbito de aplicación de la normativa 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, deben tener un SII que se regulará por su normativa específica con independencia del número de trabajadores con que cuenten (tanto en cuanto a la obliga-

ción de implantación como sus requisitos), siendo de aplicación complementaria la Ley 2/2023, en lo no previsto en la normativa específica.

- También deberán contar con canal interno de denuncias los partidos políticos, los sindicatos, las organizaciones empresariales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos.

- Las personas jurídicas privadas no obligadas, pueden voluntariamente establecer un SII. En tal caso deberá cumplir los requisitos de la Ley 2/2023.

1.4. ÁMBITO DE LOS SISTEMAS INTERNOS

1.4.1. Ámbito personal (Personas denunciantes)

- Podrán denunciar todas aquellas personas físicas que hayan tenido conocimiento de infracciones en un contexto laboral o profesional. La Ley 2/2023 incluye a trabajadores, empleados públicos, autónomos, trabajadores de contratistas, subcontratistas y proveedores, voluntarios, personal en formación (remunerado o no), y a quienes obtengan información sobre infracciones durante un proceso de selección o tras relación laboral/funcionarial finalizada.

- El ámbito personal de cada SII debe adecuarse a la naturaleza y características de cada entidad. Más allá de los empleados, se recomienda incluir en el SII a personas que, por su relación con la entidad, pueden tener acceso privilegiado a información sobre infracciones y sufren riesgo de represalias, aunque no tengan relación laboral formal (por ejemplo, colegiados en el caso de un colegio profesional, alumnos en el caso de Universidades, etc...).

- En cualquier caso, la condición del denunciante no debe ser un motivo determinante de la inadmisión de denuncias, ya que la Ley 2/2023 exige el seguimiento de denuncias anónimas, donde la identidad del denunciante y su relación con la entidad son desconocidas.

- En Andalucía, la Ley 2/2021 permite denunciar a cualquier persona, independientemente de su relación laboral con la entidad, y además impone la obligación a determinadas personas, en concreto a empleados del sector público andaluz, a comunicar cualquier infracción de la que haya tenido conocimiento.

1.4.2. Ámbito material (hechos denunciables)

- Deben posibilitar la presentación de informaciones sobre infracciones que tengan relación con la actividad y funcionamiento de la entidad:

  – Acciones u omisiones que puedan constituir infracciones del Derecho de la UE que entren dentro del ámbito de aplicación de los actos enumerados en el Anexo de la Directiva 2019/1937 (contratación pública, servicios financieros, prevención de blanqueo de capitales, etc...); afecten a los intereses financieros de la UE o Incidan en el mercado interior.

  – Acciones u omisiones que puedan ser constitutivas de infracción penal, o de infracción administrativa grave o muy grave, siempre y cuando tengan relación con la actividad y funcionamiento de la entidad.

- Podrán estar habilitados por la entidad que los gestione para la recepción de cualesquiera otras comunicaciones o informaciones fuera del ámbito establecido en la Ley 2/2023, si bien dichas comunicaciones y sus remitentes quedarán fuera del ámbito de protección dispensado por la misma.

1.5. VÍAS DECOMUNICACIÓN Y JERARQUÍA

A continuación de enumeran los aspectos más relevantes a tener en cuenta para la comunicación de información por parte de las personas denunciantes:

Canal interno, canal externo y revelación pública:

- La comunicación de información se realizará preferentemente a través de los canales internos, siempre que no existan riesgos de represalias y la infracción pueda ser tratada de manera efectiva.

- La comunicación de denuncias a través del canal interno es voluntaria, no obligatoria.

- En cualquier momento queda a salvo la posibilidad de denunciar a través del canal externo, ya sea directamente, o con posterioridad a la previa formulación de información ante el canal interno correspondiente. En Andalucía, el canal externo está gestionado por la Oficina Andaluza contra el Fraude y la Corrupción.

- La persona denunciante tiene la opción de realizar una revelación pública, que consiste en la puesta a disposición pública de información sobre acciones u omisiones relativas a infracciones tipificadas en la normativa; pudiéndose acoger a protección ante represalias si ha realizado la comunicación previamente por canales internos o externos sin que se hayan tomado medidas adecuadas, o si la infracción revelada puede constituir un peligro inminente o manifiesto para el interés público.

2. INFORMACIÓN TÉCNICA

Trataremos de exponer a continuación una forma de abordar técnicamente la implementación de un canal de denuncias a través de internet. Repasaremos primero en qué funcionalidades se traducen los requisitos normativos para después explicar una solución conforme a dichos requisitos.

2.1. FUNCIONALIDADES

Se trata de implementar la funcionalidad "Canal de denuncias" o "Canal interno" cumpliendo lo estipulado en la Directiva Europea 2019/1937 y en la norma española (Ley 2/2023), cumpliendo estos preceptos:

- Posibilidad de **mantener la comunicación con el informante.**

- Posibilidad de **solicitarle información adicional.**

- Permitir la presentación y posterior tramitación de **comunicaciones anónimas.**

- **Confidencialidad:** 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 (Art. 5.2.b).

Datos mínimos a recoger:

- 📝 Descripción de los hechos (campo libre).

- 🗓️ Fecha o periodo aproximado.

- 📍 Lugar / ámbito.

- 🧑 Personas implicadas (si se conocen).

- 📎 Subida de archivos adjuntos.

Seguimiento, anonimato y confidencialidad:

- Aportar información o acceder a respuestas.

- Sin necesidad de su identificación.

- Garantizar el anonimato:

  – No ha de exigirse autenticación ni se solicitarán ni guardarán datos identificativos.

  – No deben registrarse metadatos (IP, logs sin anonimizar...)

  – Caché (forma de programar el aplicativo)

- Garantizar la confidencialidad: Cifrado, para proteger respuestas, adjuntos, metadatos...

- Sea cual sea la modalidad de denuncia, el denunciante deberá poder consultar en la página el estado de tramitación de su denuncia.

2.2. SOFTWARE QUE PERMITE IMPLEMENTAR LOS REQUISITOS

Aunque existen otras soluciones disponibles (entre otras Whistleblowers Software ApS, Aranzadi, Lefebvre el Derecho, EQS,...etc), que ofrecen todo tipo de productos para los profesionales del Derecho y se han ocupado de cubrir esta necesidad del canal interno, existe una solución de software libre, **GlobalLeaks** que puede usarse sin coste para el organismo, y que está pensada, entre otras necesidades, para atender la implementación de un canal de denuncias, por cumplir sus requisitos legales y funcionales. Su origen fueron usos en asuntos relacionados con la protección de derechos humanos o periodismo de investigación.

- Hay abundante documentación técnica y funcional sobre la misma en la página web https://www.globaleaks.org/

- Se trata de una solución enteramente gestionable y personalizable desde el interfaz web, sin necesidad de conocimientos técnicos a bajo nivel, a no ser que se requiera un elevado nivel de personalización. Es fácil de instalar:
  - Sobre un servidor con sistema operativo Ubuntu o Debian.
  - Contenedores Docker.
- Cuenta con un plan de soporte a medio y largo plazo (LTS), mediante un canal de soporte del producto, por lo que bugs o fallos que aparecen, se irán resolviendo.
- Permite varios roles diferenciados:
  - Los 2 principales son Receptor o destinatario (las personas encargadas de tramitar y dar cauce a las denuncias recibidas) y administrador (personal de TI del organismo).
  - Otros roles: Custodio y analista (estadísticas).
- Permite la navegación con los navegadores habituales y, adicionalmente, permite la navegación con el navegador TOR, lo que evitará que terceras partes, en el trayecto digital, puedan contar con logs o rastro de la dirección IP o la URL a la que se conecta el denunciante. Utilizando este navegador queda garantizada la **navegación anónima** extremo a extremo, por cubrir también aquellos tramos digitales anteriores al acceso a la propia página.
- Permite desde su interfaz la personalización de campos de formularios (cuestionarios) sin conocimientos técnicos amplios: Campos de texto, combos, subida de ficheros… También permite introducir validaciones web mediante el uso de javascript.
- Permite múltiples formatos de archivo: pdf, .zip, jpeg, mp3, ogg, wav, mp4… Existe también la opción de configurar un campo de formulario tipo voz (permitiría denuncias verbales).
- Seguimiento con **código** que recibe de la página en el momento de presentación de la misma (y que sólo conoce él), pudiendo aportar información adicional en cualquier momento o acceder a la documentación que se vaya incorporando a su expediente por parte de los gestores. En ambas modalidades utilizando mecanismos de cifrado para la protección del formulario.
- Permite la notificación de emails cifrados, distinguiendo entre cifrado en tránsito (TLS) y cifrado de contenido extremo a extremo mediante OpenPGP (Gestores).
- Respecto a la capacidad de flujos de trabajo, lo que permite es repartir las denuncias, mediante dos modalidades, transferencia (pasa otra persona a encargarse) y conceder acceso (se añade otro gestor).
- Cuenta con mecanismos de recuperación de claves que garantizan la salvaguarda o pérdida de datos en caso de pérdida de la clave de usuario. Los usuarios (los receptores o gestores de denuncias) pueden acceder a su propia clave de recuperación pinchando en el botón presente en su página de preferencias. Es un paso fundamental que debe hacer todo usuario después de activarse su cuenta para guardar dicha clave y asegurarse así que no dejarán de tener acceso si olvidan la contraseña.
- Cuenta con un sistema de cifrado robusto que garantiza la confidencialidad de la información aportada por los usuarios (cifrado PEM, y certificado digital autogenerado tipo Let's encrypt —entidad certificadora).
- Permite la autenticación mediante dos factores para los gestores de las denuncias, de forma que se minimice el riesgo de suplantación de su identidad (es configurable). Sólo requiere la instalación en su teléfono de una aplicación común de autenticación.

Recomendaciones:

- Es recomendable que este software se instale en un servidor dedicado en exclusiva al mismo. Ello no impide que se pueda integrar en cualquier página web sin más que enlazar ésta a dicho módulo y aplicar, a este aplicativo el diseño (plantillas) definido para la web del organismo.
- Es útil el filtrado por IP que incorpora para los gestores definidos.
- Es posible probar la solución incluso previamente a su instalación por el organismo, puesto que la web de GlobalLeaks ofrece una demo gratuita donde se ofrece usuario y contraseña de administrador para configurar online un buzón de denuncias alojado en la nube: https://try.globaleaks.org/#/
- Es recomendable que la web del canal de dee nuncias ofrezca aviso al usuario sobre la recomendación de utilización del navegador TOR, dado que su utilización impide que alguien conozca los sitios web que se visitan, bloquea rastreadores, dada su resistencia a la identificación unívoca (para evitar la identificación por navegador y dispositivo) y su cifrado en múltiples capas.
- Dado que no es posible acceder al contenido interno de las denuncias por los administradores de TI, es conveniente contar, como mecanismo ante problemas técnicos graves, con copias de seguridad frecuentes:
  - La copia incluirá toda la configuración y los datos.
  - La política de copias de seguridad es conveniente que incluya una copia diaria completa, guardada en sitio encriptado.
  - Existe un comando (gl-admin backup) que permite realizar el backup de todo lo que es relevante en globaleaks. Puede incluirse en el cron diario, que también debe incluir la subida al backend de almacenamiento de las copias.
- Ha de personalizarse el tiempo de caducidad de las denuncias mediante un parámetro que fija los días de caducidad, de forma que haya tiempo suficiente para la tramitación del expediente. Además, permite modificar (y por tanto ampliar) dicho número de días si, durante la tramitación, se estima necesario.
- Personalización del diseño de Globaleaks
  Ofrece diseño responsive: acceso desde cualquier tipo de dispositivo, sea móvil, tablet, portátil o pc.

  Cabe preguntarse si, al ser un aplicativo diferente a la web corporativa del organismo, es posible adaptar o personalizar la apariencia e interfaz de usuario. A este respecto, cabe indicar:
  - Es posible adaptar la apariencia de la plataforma al "look and feel" de la web corporativa mediante funcionalidades de configuración (subir el logo del organismo, favicon…), el uso de ficheros CSS y Javascript, desde el interfaz de administración.
  - Como consideraciones adicionales, es aconsejable realizar una copia de seguridad de la configuración y los archivos originales, por si es necesario revertir los cambios y asegurarse de que el código CSS y JavaScript es compatible con las versiones de los navegadores utilizados por los usuarios de la plataforma, además de revisar el código JavaScript para evitar posibles vulnerabilidades de seguridad.
  - Validación de longitud o de expresiones ree gulares desde el propio interfaz, y validaciones adicionales mediante javascript (ej. DNI).

OFICINA **ANDALUZA** ANTIFRAUDE

Edificio Cepeda
C/ Carlos de Cepeda nº2, 1ª planta, módulo 3
41005 Sevilla
www.antifraudeandalucia.es