

SISTEMA INTERNO DE INFORMACIÓN (SII)

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

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

ELEMENTOS:

1. Política o estrategia que enuncie principios generales

Deben enunciarse los principios generales del Sistema interno de información y defensa de la persona informante y ello debe ser publicitado en el seno de la entidad u organismo.

A modo de ejemplo, estos son los principios que deben inspirar la configuración y el funcionamiento del Sistema interno de informaciones, así como el tratamiento de la información recibida:

- Accesibilidad: Facilidad de acceso al canal y visibilidad del mismo, que incluya una navegación y tramitación intuitiva para los distintos usuarios destinatarios.
- Bidireccionalidad: Permitir en cualquier momento la comunicación entre las personas intervinientes.
- Agilidad: A disposición de las personas informantes medios de comunicación de uso sencillo y con plazos breves de respuesta.
- Celeridad: Con plazos breves para poder adaptar las medidas que se consideren oportunas.
- Confiabilidad: Con medidas que garanticen la confidencialidad y el anonimato de las personas y las informaciones recibidas.
- Privacidad: El tratamiento de datos personales se realizará de acuerdo con la legislación vigente en la materia.
- Claridad comunicativa: Que se pueda comprender teniendo en cuenta el usuario destinatario.
- Efectividad: El canal deber estar configurado de forma que las comunicaciones que se presenten se traten en primer lugar y de forma directa por el Responsable del Sistema.
- Independencia: El Responsable del Sistema debe desarrollar sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad u organismo. Debe disponer de todos los medios personales y materiales necesarios para llevarlas a cabo y no recibir instrucciones de ningún tipo en su ejercicio.

2. Canal interno de información

La persona informante puede elegir presentar la comunicación a través del canal interno de la entidad donde presta servicios o del canal externo, aunque se reconoce carácter preferente a la utilización del SII.

En ambos canales se aplicarán las siguientes reglas:

- **Deber de confidencialidad**. Las actuaciones deben asegurar la reserva máxima para evitar perjuicios a la persona o entidad investigada y como salvaguarda de la eficacia del procedimiento.
- El**tratamiento de datos personales**, incluido el intercambio o transmisión de estos datos entre autoridades competentes, se debe realizar de conformidad con su normativa reguladora.

El canal interno de Información es la herramienta informática integrada en el SII de cada entidad u organismo, que debe cumplir con los siguientes requisitos:

- Permitir comunicaciones escritas o verbales, identificadas o anónimas.
- Tener carácter bidireccional, permitiendo la posible interacción entre el Responsable del Sistema y las personas informantes.
- Aparecer diferenciado y de forma independiente al resto de canales internos, si los hubiera.
- Todas las informaciones o comunicaciones quedarán registradas en un libro-registro.
- Se recomienda la implementación del software libre y gratuito basado en la herramienta https://www.globaleaks.org, certificada conforme a la ISO 2001 https://www.whistleblowingsolutions.it/docs/en/certificate-iso-27001.pdf, que cumple con las exigencias de confidencialidad, registro de denuncias y tratamiento de datos personales, fijadas por la Directiva 2019/1937(UE) y por la Ley 2/2023.
- Situarse en un lugar visible de la página web o cualquier otro soporte, incluyendo el link al canal externo de denuncias, que para el sector público de la Comunitat Valenciana es el*Buzón de denuncias de la AVAF* , junto con información clara y precisa acerca de su función y finalidad.

3. Responsable del SII

Su función principal es la tramitación diligente de las comunicaciones recibidas por el canal interno, lo que deberá desarrollar de forma independiente y autónoma, sin recibir instrucciones de ningún tipo, debiendo disponer de todos los medios personales y materiales necesarios para llevarlas a cabo.

La Ley 2/2023 no determina un perfil (requisitos y conocimientos) que debe cumplir el Responsable del Sistema, las únicas pistas que indica lo son para el caso del sector privado, que podrá ser un directivo de la entidad, que ejercerá su cargo con independencia, pudiendo en determinados casos compatibilizar las funciones de Responsable del Sistema con el desempeño ordinario de otras funciones del puesto o cargo. También, con carácter general, se indica que, en el caso que ya existiera una persona responsable de la función de cumplimiento normativo o de políticas de integridad, podrá ser esta la persona designada como Responsable del Sistema. De ello se deriva que para el buen funcionamiento del SII será imprescindible implicar en su gestión a personal que cuente con la debida formación, experiencia en tareas de responsabilidad y conocimientos específicos.

Una vez designado el Responsable del Sistema interno de información (persona física u órgano colegiado) por el órgano de administración u órgano de gobierno de cada entidad u organismo obligado por la Ley 2/2023, este **deberá ser notificado** a las autoridades u órganos competentes de las comunidades autónomas.

En la Comunitat Valenciana, respecto a las administraciones y entidades incluidas en el ámbito subjetivo de aplicación de la Ley 11/2016, el nombramiento del Responsable del Sistema y, en su caso, cese motivado deberá notificarse ante la AVAF. Al efecto, se aprobó la Resolución núm. 504/2023, de 10 de mayo, por la que se crea el Registro de Responsables de Sistemas Internos de Información y se regula su funcionamiento (DOGV núm. 9601, 23.05.2023).

La notificación del nombramiento de dicho Responsable o su cese motivado debe realizarse en el plazo de los diez días hábiles siguientes.

El trámite específico en nuestra sede electrónica se encuentra en el apartado “Trámites destacados”: https://sede.antifraucv.es/carpetaciudadana/tramite.aspx?idtramite=16811. Se debe cumplimentar el formulario y remitir copia del acuerdo o resolución de designación.

4. Procedimiento de gestión de informaciones

Otro de los elementos fundamentales con el que debe contar todo Sistema interno de información (SII) es el procedimiento de gestión de las informaciones recibidas a través del canal interno, de cuya tramitación diligente responderá el Responsable del Sistema.

Este procedimiento debe ser aprobado por el órgano de administración u órgano de gobierno de cada entidad u organismo obligado por la ley y se regula en el artículo 9 de la Ley 2/2023.

El **contenido mínimo** de dicho procedimiento y los principios que deben regir el mismo, de manera sucinta, son los siguientes:

A continuación, se transcribe, a modo de ejemplo, un procedimiento genérico de gestión de informaciones obtenidas a través del canal interno:

MODELO GENÉRICO DE PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES

1. Presentación de comunicaciones

Las comunicaciones se deberán realizar por escrito o verbalmente (habilitándose la herramienta adecuada al efecto), o bien de ambas formas. La comunicación podrá presentarse de forma identificada o anónima, a elección de la persona informante, garantizándose en cualquier caso la reserva de su identidad.

La garantía de confidencialidad se extenderá a la identidad de la persona informante y de la/s posible/s persona/s afectada/s por la información, y se mantendrá a lo largo de todo el procedimiento de gestión y respecto de cualquier actuación o dato derivado de su tramitación, incluso una vez terminado el procedimiento.

Cualquier persona que, sin ser responsable de la tramitación de la comunicación, la reciba, indistintamente del motivo, deberá guardar secreto de la misma y remitirla de manera inmediata al Responsable del Sistema. El quebranto de este deber de confidencialidad está tipificado como infracción muy grave.

Los tratamientos de protección de datos personales que se deriven del presente procedimiento se regirán por la normativa vigente en la materia y por lo dispuesto en el título IV de la Ley 2/2023.

En el Canal Interno de Informaciones de la Ley 2/2023 se podrán presentar comunicaciones que versen sobre acciones u omisiones relacionadas con el funcionamiento de la organización que puedan ser constitutivas de infracciones del Derecho de la Unión Europea siempre que cumplan los requisitos señalados en la citada ley o de infracciones penales o administrativas graves o muy graves.

Se especificarán también otros canales internos habilitados por la organización, los cuales en caso de existir quedan integrados en su Sistema interno de información.

El canal externo de información de la Ley 2/2023 en la Comunitat Valenciana es la Agencia de Prevención y Lucha contra el fraude y la Corrupción de la Comunitat Valenciana, respecto a las entidades incluidas en su ámbito de actuación (artículo 3 de la Ley 11/2016, de 28 de noviembre, de la Generalitat). Se puede acceder al Buzón de Denuncias de la Agencia a través del siguiente link: https://www.antifraucv.es/buzon-de-denuncias-2/

Además, se incluirá información sobre los demás canales externos de información existentes. A título de ejemplo, Servicio Nacional de Coordinación Antifraude, Tribunal de Cuentas, Oficina Europea de Lucha contra el Fraude, Inspección de Trabajo, Comisión Nacional de los Mercados y la Competencia u órgano competente a nivel autonómico, AEAT u órgano competente a nivel autonómico o nacional, Fiscalía o Fiscalía Europea, Síndic de Greuges, etc.

2. Recepción de la información

Recibida una comunicación a través del canal interno de información de la Ley 2/2023, se procederá a su registro mediante la asignación de un código de identificación. A continuación, se enviará el correspondiente acuse de recibo en el plazo de siete días naturales siguientes a su recepción, salvo que sea contrario a la confidencialidad.

La presentación de una comunicación por el informante no le confiere, por sí sola, la condición de interesado.

3. Valoración y trámite de admisión

Por el Responsable del Sistema se realizará un análisis preliminar para determinar si los hechos relatados entran dentro del ámbito de aplicación de la Ley 2/2023 y se valorará la competencia, la verosimilitud de la información presentada y la suficiencia de las evidencias aportadas.

En los casos en que la comunicación aportada presente alguna carencia de información, se podrá efectuar el correspondiente requerimiento.

Realizada esta comprobación, se decidirá en el plazo de diez días hábiles desde la fecha de entrada en el registro de la información sobre los siguientes extremos:

- Inadmisión a trámite de la comunicación.
- Admisión a trámite de la comunicación.
- Remisión con carácter inmediato de la información a la autoridad judicial o al Ministerio Fiscal cuando los hechos pudieran ser indiciariamente constitutivos de delito, o a la Fiscalía Europea en caso de afectar los intereses financieros de la Unión Europea.
- Remisión a otra autoridad, entidad u organismo que se considere competente para su tramitación.

La decisión se comunicará a la persona informante dentro de los cinco días hábiles siguientes, salvo cuando este hubiera renunciado a recibir comunicaciones. Dicha comunicación de la decisión se realizará a través de canal interno de informaciones, que deberá permitir la interacción con la persona informante (bidireccionalidad).

Procederá la inadmisión a trámite de la comunicación en los siguientes supuestos:

1º. Cuando los hechos relatados carezcan de toda verosimilitud.

2º. Cuando la comunicación carezca manifiestamente de fundamento o de contenido esencial, cuando sea notoriamente falsa, o esté fundada únicamente en opiniones o formulada de forma vaga o excesivamente genérica.

3º. Cuando los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico incluida en el ámbito de aplicación de la Ley 2/2023.

4º. Cuando existan indicios racionales de que la comunicación se ha obtenido mediante la comisión de un delito, en cuyo caso, además de la inadmisión, se remitirá al Ministerio Fiscal relación circunstanciada de los hechos.

5º. Cuando sea manifiestamente repetitiva, salvo que se aprecien nuevas circunstancias de hecho o de derecho que justifiquen una nueva valoración. Se entenderá que concurre esta causa cuando no se contenga información nueva y significativa respecto de anteriores comunicaciones previamente inadmitidas o debidamente investigadas.

6º. Cuando esté siendo investigada por la autoridad judicial.

4. Instrucción

Se realizarán todas aquellas actuaciones encaminadas a comprobar la exactitud y veracidad de la información recibida. Dicha comprobación se efectuará por el Responsable del Sistema, sin perjuicio de que en función de los hechos comunicados se pueda requerir la colaboración de otras personas o unidades administrativas de la entidad, quienes en todo caso deberán guardar deber de sigilo y confidencialidad.

Se garantizará que la persona afectada por la información tenga noticia de los hechos relatados, sin que en ningún caso se identifique la persona informante ni se dé acceso a la comunicación o denuncia. Asimismo, se informará a la persona afectada de sus derechos: a presentar alegaciones por escrito, a ser oída en cualquier momento, de acceso al expediente y al tratamiento de sus datos personales. No obstante, el derecho de acceso tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.

Sin perjuicio del derecho a formular alegaciones por escrito, la instrucción comprenderá, siempre que sea posible, una entrevista con la persona afectada en la que, con absoluto respeto a la presunción de inocencia, se le invitará a exponer su versión de los hechos y a aportar aquellos medios de prueba que considere adecuados y sean pertinentes.

Durante todo el procedimiento se garantizará a la persona afectada la misma protección establecida para las personas informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento. Asimismo, se actuará con especial sensibilidad a la presunción de inocencia y al honor de las personas afectadas.

5. Terminación

Una vez finalizadas las actuaciones de instrucción correspondientes, el Responsable del Sistema emitirá un informe que elevará al órgano competente.

El referido informe debe incluir al menos:

a) Una exposición de los hechos relatados, el código de identificación de la comunicación y la fecha de registro.

b) La clasificación de la comunicación a efectos de conocer la prioridad o no en su tramitación.

c) Las actuaciones realizadas para comprobar la verosimilitud de los hechos.

d) Las conclusiones de la instrucción y la valoración de las diligencias y de los indicios que las sustentan.

Recibido el informe, el órgano competente adoptará una de las siguientes decisiones:

a) Archivo del expediente.

b) Remisión a la autoridad judicial, al Ministerio Fiscal o a la Fiscalía Europea.

c) Traslado de lo actuado al órgano competente.

d) En el caso de que los hechos pudieran ser constitutivos de una infracción grave o muy grave cometida por personal de la entidad, orden de apertura del procedimiento sancionador o disciplinario correspondiente o de las actuaciones previas a este.

El plazo máximo para dar respuesta a la persona informante de las actuaciones de investigación no podrá ser superior a tres meses a contar desde la recepción de la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso este podrá extenderse hasta un máximo de otros tres meses más.

En caso de información o denuncia notoriamente falsa, tergiversada u obtenida de manera ilícita, se exigirán las responsabilidades legales que procedan.

El resultado de las actuaciones se comunicará a la persona informante, así como a la persona afectada en el caso que hubiera tenido noticia de la comunicación o denuncia.

Las decisiones adoptadas no serán recurribles en vía administrativa ni en vía contencioso-administrativa, sin perjuicio del recurso administrativo o contencioso-administrativo que pudiera interponerse frente a la eventual resolución que ponga fin al procedimiento sancionador o disciplinario.

6. Revisión del procedimiento

El procedimiento de gestión de informaciones se revisará, al menos, una vez cada tres años, a fin de incorporar actuaciones y buenas prácticas que conforme a la experiencia acumulada sirvan para su mejora. La modificación del procedimiento será objeto de la debida publicación.

5. Derechos y garantías de las personas informantes y de las personas afectadas

Nota: Diferencias entre el canal interno de información y otras figuras.

Canal interno de información

Herramienta integrada en el Sistema interno de información regulado por la Ley 2/2023, que transpone la Directiva (UE) 2019/1937. Es obligatorio para todo el sector público en toda su extensión y para el sector privado salvo empresas que cuenten con menos de 50 trabajadores. Debe permitir la presentación de información de forma anónima y garantizar la confidencialidad.

Canal ético y comités éticos

Medio para reportar cualquier vulneración del código ético o de conducta de la empresa, entendido como el conjunto de normas, pautas, líneas de actuación y valores corporativos formulados a través de una serie de principios acordados desde la propia organización y que constituyen la base fundamental de su normativa interna. Los canales éticos cobraron importancia tras la introducción del artículo 31 bis en el Código Penal, convirtiéndose en un medio para que las empresas puedan atenuar o eximir su responsabilidad penal en la comisión de determinados delitos por parte de sus miembros. Forma parte del sistema de gestión de compliance y está a disposición de cualquier miembro de la empresa, incluido el personal directivo. En el ámbito privado, la propia Ley 2/2023 señala que pueden acometer sus fines los compliance officer de las empresas.

Comités antifraude

En cumplimiento de la Orden HFP/1031/2021, de 29 de septiembre, del Plan de Recuperación, Transformación y Resiliencia. El comité antifraude es el órgano colegiado responsable de realizar, supervisar y aprobar la evaluación de riesgo a los intereses financieros de la Unión, y de proponer medidas correctoras y de mejora de los procedimientos relativos a la prevención, detección, corrección y persecución del conflicto de interés, el fraude y la corrupción de los fondos europeos. Existe un canal de denuncias externo para comunicar informaciones sobre fraude, corrupción o cualquier otra actividad ilegal que afecte a fondos europeos que gestiona el Servicio Nacional de Coordinación Antifraude (SNCA), adscrito a la IGAE. Dicho Servicio Nacional facilita la coordinación efectiva y el intercambio de información con la OLAF. En la práctica está siendo frecuente que estos comités antifraude asuman los SII incorporándoles las funciones de la Ley 2/2023.

Quejas y sugerencias

De conformidad con el artículo 38.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y del artículo 11.2.b) del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, cada administración pública garantizará a través de su Sede Electrónica el acceso los medios disponibles para la formulación de sugerencias y quejas. El objeto de este trámite es ofrecer a los ciudadanos un canal de comunicación para que formulen aquellas quejas y sugerencias que estimen oportunas.

Fuente: antifraucv.es

1. Identificación de los canales internos.
2. Información clara y accesible sobre los canales externos.
3. Acuse de recibo de la comunicación a la persona informante de siete días naturales.
4. Plazo máximo para dar respuesta a las actuaciones de investigación no superior a tres meses, salvo casos de especial complejidad en los que podrá extenderse hasta tres meses más.
5. Mantenimiento de la comunicación con la persona informante y, en su caso, solicitud de información adicional.
6. Derecho de la persona afectada a que se le informe de las acciones u omisiones que se le atribuyen y a ser oída en cualquier momento.
7. Garantía de confidencialidad y tipificación como infracción muy grave del quebranto del deber de secreto.
8. Presunción de inocencia y derecho al honor de las personas afectadas.
9. Cumplimiento de la normativa sobre protección de datos personales.
10. Remisión inmediata de la información al Ministerio Fiscal (o Fiscalía Europea) cuando hubiera indicios de delito.

1. **POLÍTICA O ESTRATEGIA**
2. **CANAL**
3. **RESPONSABLE**
4. **PROCEDIMIENTO**
5. **GARANTÍAS**