

**CAJA DE AHORROS Y MONTE DE PIEDAD DE ONTINYENT**

**Procedimiento de gestión de informaciones**  
Sistema interno de información

Ontinyent, noviembre 2023

## ÍNDICE

1. Introducción .....	3
2. Finalidad y ámbito de aplicación .....	3
3. Definiciones.....	4
4. Principios Generales .....	5
4.1 Derechos de los informantes .....	5
4.2 Derechos de las personas afectadas.....	5
5. Registro y documentación de las informaciones .....	6
6. Identificación de canales de información.....	6
6.1 Canal interno de información.....	6
6.2 Recepción de información por personas ajenas al Responsable del Sistema.	7
6.3 Canal externo de información de las autoridades competentes .....	7
7. Procedimiento de gestión de informaciones .....	8
7.1 Requisitos formales de la comunicación .....	8
7.2 Plazos del procedimiento .....	9
8. Fases del procedimiento .....	9
8.1 Recepción de informaciones.....	9
8.2 Fase de admisión .....	10
8.3 Fase de investigación o instrucción.....	11
8.4 Fase de resolución o finalización .....	12
9. Protección de datos personales .....	13
10. Medidas de protección al informante .....	14
11. Control de versiones.....	15

## 1. Introducción

El 21 de febrero de 2023 se publicó en el Boletín Oficial del Estado 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 (en adelante, la “**Ley 2/2023**”). Con esta aprobación se incorpora al Derecho español la Directiva (UE) 2019/1937 del Parlamento y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.

La referida Ley 2/2023, de conformidad con la Directiva, tiene como finalidad la protección de las personas que en un contexto laboral o profesional detecten determinadas infracciones penales o administrativas graves o muy graves y las comuniquen mediante los canales internos de información que deberán habilitarse al respecto, otorgando una protección adecuada frente a cualquier tipo de represalias.

En cumplimiento de dicha ley, en noviembre de 2023 el Consejo de Administración de **CAIXA ONTINYENT** (en adelante la “**Entidad**”) ha aprobado la implantación del *Sistema interno de información y defensa del informante* que tiene como objetivo definir los principios y premisas que regulan dicho sistema, el cual se configura como una herramienta para fortalecer la cultura de la información/comunicación como mecanismo esencial para la prevención, detección y corrección de incumplimientos normativos, consolidar el marco de supervisión del riesgo de cumplimiento y facilitar el cumplimiento de su normativa interna en particular.

Así mismo, de acuerdo con el artículo 9 de la Ley 2/2023, el Consejo de Administración de la Entidad debe aprobar el procedimiento de gestión de informaciones.

## 2. Finalidad y ámbito de aplicación

El presente *Procedimiento de gestión de informaciones* tiene la finalidad de establecer las previsiones necesarias para que el *Sistema interno de información* de la Entidad y las vías de comunicación para remitir la información cumplan con los requisitos establecidos en la Ley 2/2023.

En cuanto al ámbito de aplicación, la Ley prevé:

- cualquiera de las acciones u omisiones que puedan constituir infracciones del derecho de la Unión Europea,
- acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave,
- que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social,
- y la protección prevista para las personas trabajadoras que informen sobre infracciones del derecho laboral en materia de seguridad y salud en el trabajo.

La Ley protege a las personas frente a posibles represalias. Entre otras:

- Personas que tienen vínculos profesionales o laborales con la Entidad (personal empleado, miembros de los órganos de gobierno, colaboradores, proveedores y personas que trabajen para o bajo su supervisión).

- Aquellas que ya han finalizado su relación profesional.
- Trabajadores en prácticas o en periodos de formación.
- Personas que participan en procesos de selección.
- Personas que prestan asistencia a los informantes y personas de su entorno que pueden sufrir represalias.
- Personas jurídicas propiedad del informante.

### 3. Definiciones

A los efectos de la presente regulación se entenderá por:

1.- Informante: persona física o jurídica que haya obtenido información sobre infracciones en un contexto laboral o profesional y que las pongan en conocimiento de la Entidad, comprendiendo en todo caso las previstas en el artículo 3 apartados 1 y 2 de la Ley 2/2023.

2.- Persona afectada: persona física a la que se atribuye por el informante la comisión de las infracciones a las que se refiere el artículo 2 de la Ley 2/2023. También se considerarán personas afectadas, las que, sin haber sido objeto de información por el informante, a través de los actos de instrucción del procedimiento se haya tenido conocimiento de la presunta comisión por parte de éstas de las infracciones antes referenciadas.

3.- Terceros: personas físicas que pueden tener conocimiento de aspectos relacionados con la infracción informada, ya sea como testigo directo o indirecto y que puede aportar información al procedimiento.

4.- Sistema interno de información (SII): es el cauce de información establecido en la Entidad para informar sobre las acciones u omisiones previstas en el artículo 2 de la Ley 2/2023, con las funciones y contenidos recogidos en el artículo 5.2 de dicha norma.

Incluye el Canal interno de información el Responsable del SII, una Política que define los principios generales de actuación y un Procedimiento de gestión.

5.- Canal interno de información: Medios específicamente habilitados por la Entidad para recibir la información.

6.- Canal externo de información: Otros canales de información, alternativos al canal interno, con el fin de ofrecer una comunicación con una autoridad pública especializada.

7.- Responsable del SII: Persona física responsable de la gestión de todo el SII. El nombramiento, destitución o cese lo realizará el Consejo de Administración de la Entidad. No puede recibir instrucciones de ningún otro órgano o unidad de la Entidad. Es independiente en el ejercicio de sus funciones.

8.- Gestor delegado: persona designada por el Responsable del Sistema que llevará a cabo las acciones oportunas para determinar la verosimilitud de las informaciones recibidas y la gestión del expediente, y dará cuenta al Responsable del Sistema de las actuaciones llevadas a cabo así como de cualquier información que este le solicite.

9.- Sistema de gestión de la Información: plataforma tecnológica integrada en el SII, cuya finalidad es la llevanza, registro y conservación de las actuaciones que tengan lugar como consecuencia de la presentación de una información a la que sea aplicable la Ley 2/2023. Se encuentra bajo la administración del Responsable del SII.

## 4. Principios Generales

### 4.1 Derechos de los informantes

1. A los informantes se les garantizarán el efectivo ejercicio de los siguientes derechos, sin perjuicio de cualesquiera otros que les reconozcan la Constitución y las leyes:

- a) A presentar informaciones de modo anónimo y a que se mantenga el anonimato durante el procedimiento.
- b) A indicar un domicilio, correo electrónico o lugar seguro donde recibir las comunicaciones que realice el Responsable del Sistema.
- c) A comparecer ante el Responsable del Sistema o el gestor delegado por iniciativa propia.
- d) A la preservación de su identidad.
- e) A la protección de sus datos personales.
- f) A conocer la identidad del gestor delegado que instruya el procedimiento.
- g) A la confidencialidad de las comunicaciones.
- h) A las medidas de protección y de apoyo en los términos previstos en la Ley 2/2023.
- i) A presentar reclamación ante la Autoridad Independiente de Protección del Informante.

2. A los terceros en el procedimiento se les reconocen los derechos previstos en las letras b), c), d), e) y g) del apartado 1. Sin perjuicio de la posibilidad de extender a éstos, y en la medida de lo posible, las medidas de apoyo y protección del informante previstas en la Ley 2/2023.

### 4.2 Derechos de las personas afectadas

Las personas afectadas tienen los derechos que les reconozcan la Constitución y las leyes, debiendo estar garantizados por el Responsable del Sistema, y en especial los siguientes:

- a) A ser informadas a la mayor brevedad posible de la información que les afecta.
- b) Al honor y a la intimidad.
- c) A la presunción de inocencia, y a usar todos los medios válidos en derecho para su defensa.
- d) A ser asistidas por abogado.
- e) Al acceso a las actuaciones que se siguen contra ellos, sin perjuicio de las limitaciones temporales que se pueden adoptar para garantizar el resultado de las actuaciones.
- f) A conocer la identidad del gestor delegado que instruya el procedimiento.

- g) A la preservación de su identidad, frente a cualquier persona ajena al Responsable del Sistema.
- h) A la protección de sus datos personales.
- i) A la confidencialidad de las comunicaciones.

## 5. Registro y documentación de las informaciones

1. Sin perjuicio del registro de informaciones al que se refiere el artículo 26 de la Ley 2/2023, la presentación de información se documentará, en su caso, por los siguientes medios:

- a) Mediante la copia del escrito de presentación de la información.
- b) Mediante una grabación de la conversación en un formato seguro, duradero y accesible.
- c) A través de una transcripción completa y exacta de la conversación mantenida en la reunión presencial, que se hará constar en el Acta correspondiente. En este supuesto, se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

2. La documentación de las informaciones a las que hace referencia el apartado anterior se incorporarán en el sistema de gestión de la información.

## 6. Identificación de canales de información

El SII de la Entidad integra el canal interno de información, lo que permite garantizar en todas las vías de acceso allí previstas que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la Entidad, con el objetivo de que sea esta la primera en conocer la posible irregularidad.

### 6.1 Canal interno de información

El Canal interno de información de la Entidad es la vía principal para posibilitar la presentación de información respecto de posibles infracciones por actos o conductas, presentes o pasadas, que puedan suponer un incumplimiento de la Guía Ética de Conducta del Personal de Caixa Ontinyent u otras normas de conducta relacionadas en la *Política del sistema interno de información y defensa del informante* de la Entidad.

Las comunicaciones pueden presentarse de forma nominativa, es decir, con identificación del informante, o de forma anónima.

Este Canal permite la presentación de comunicaciones a través de:

- <https://www.caixaontinyent.es/canal-interno>
- Correo electrónico: [canal-interno@caixaontinyent.es](mailto:canal-interno@caixaontinyent.es).
- Correo postal: Pza. Sant Domingo, 24 - 46870, Ontinyent (Att. Responsable del Sistema Interno de Información).

- A solicitud de la persona informante las comunicaciones también pueden presentarse mediante reunión presencial, dentro del plazo máximo de siete días, debiendo para ello dirigir la petición a través de alguna de las vías de comunicación mencionadas anteriormente.

Las comunicaciones verbales, realizadas a través de reunión presencial previo consentimiento del informante, serán documentadas:

- a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla, ofreciendo al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación; o
- mediante una grabación de la conversación en un formato seguro, duradero y accesible; en cuyo caso, se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo con lo que establece el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

## 6.2 Recepción de información por personas ajenas al Responsable del Sistema

Cuando la información no se remita a través del Canal interno de información y llegue a miembros de la Entidad distintos del Responsable del Sistema, éstos tienen la obligación de remitírsela con carácter inmediato, así como el deber de preservar su confidencialidad y abstenerse de realizar cualquier actuación que pueda revelar directa o indirectamente la identidad del informante y de la persona afectada.

A estos efectos, la Entidad llevará a cabo acciones formativas para su personal en esta materia.

La divulgación por parte del tercero receptor de la mera existencia y, en su caso, del contenido de la información, puede suponer la vulneración de las garantías de confidencialidad y anonimato, conducta tipificada como infracción muy grave en el artículo 63.1. c) de la Ley 2/2023.

## 6.3 Canal externo de información de las autoridades competentes

Sin perjuicio del acceso al Canal interno detallado, y en cualquier momento, toda persona física que forme parte de algunos de los colectivos con acceso al SII puede dirigirse a la **Autoridad Independiente de Protección del Informante (A.A.I.)** o ante las autoridades u órganos autonómicos correspondientes, para informar de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación de la Ley 2/2023.

Exponemos a continuación las principales autoridades competentes que disponen de canales de comunicación externos:

- Autoridad Independiente de Protección del Informante<sup>1</sup>.
- Banco de España, a través del siguiente enlace: [Banco de España Canal Externo | Inicio \(integrityline.com\)](#)
- Comisión Nacional del Mercado de Valores, a través del siguiente enlace, [CNMV - Comunicación de posibles infracciones en el ámbito de los mercados de valores](#)
- Agencia Española de Protección de Datos, a través del siguiente enlace, [Canal de protección del informante | AEPD](#)

## 7. Procedimiento de gestión de informaciones

El presente marco de gestión se basa en los principios y garantías del SII de la Entidad, cuyo detalle se encuentra en la *Política del sistema interno de información y defensa del informante*.

Las gestiones se llevarán a cabo de manera personalizada y en colaboración con las partes involucradas, manteniendo un registro documental de todas las acciones realizadas.

### 7.1 Requisitos formales de la comunicación

1. Sin perjuicio del modo de presentación de la información a través del Canal interno de información, la comunicación deberá contener al menos los siguientes requisitos:

- a) Identificación del informante. Salvo que se presente la información de modo anónimo.
- b) Descripción de los hechos y en su caso, determinación de la norma afectada.
- c) Posibilidad de identificación de la persona o personas afectadas.
- d) Posibilidad de identificación, en su caso, de terceros que puedan aportar información relevante.

2. Al presentar la información, el informante podrá indicar un domicilio, correo electrónico, o lugar seguro a efectos de recibir las comunicaciones.

3. En caso de apreciarse por el Responsable del Sistema o gestor delegado la falta de alguno de los requisitos que se acaban de indicar, se procederá en la medida de lo posible, a solicitar la subsanación. Esta subsanación también podrá realizarse a petición del informante mediante la comunicación ante el Responsable del Sistema o el gestor delegado.

---

<sup>1</sup> Organismo actualmente no existente. Según la disposición final undécima de 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. su creación deberá llevarse a cabo en el plazo de un año desde la entrada en vigor de esta ley, es decir, el 13 de marzo de 2024, el Consejo de Ministros, aprobará mediante real decreto, a propuesta conjunta de los Ministerios de Justicia y de Hacienda y Función Pública, el Estatuto de la Autoridad Independiente de Protección del Informante, A.A.I., en el que se establecerán las disposiciones oportunas sobre organización, estructura, funcionamiento, así como todos los aspectos que sean necesarios para el cumplimiento de las funciones asignadas mediante esta ley.



## 7.2 Plazos del procedimiento

1. El plazo para resolver las actuaciones de investigación a las que da lugar el procedimiento de gestión de informaciones no puede ser superior a 3 meses, salvo supuestos de especial complejidad en cuyo caso podrá, motivadamente, acordarse la ampliación de dicho plazo por el Responsable del Sistema hasta un máximo de otros tres meses adicionales.

2. El cómputo del plazo al que se refiere el apartado anterior se inicia desde la recepción de la comunicación por parte del Responsable del Sistema o, si no se remite un acuse de recibo al informante, desde el vencimiento del plazo de siete días después de haberse recibido la comunicación.

Los plazos expresados en meses se computarán de fecha a fecha.

3. Los plazos en días a los que se hace referencia en el presente procedimiento se considerarán hábiles, salvo que expresamente se indique que son naturales.

## 8. Fases del procedimiento

A continuación, se muestran las distintas fases del proceso de gestión de las comunicaciones:

### 8.1 Recepción de informaciones

1. Como ya se ha indicado, la información podrá realizarse por escrito, mediante correo postal o de manera telemática a través de la aplicación habilitada al efecto. También, a solicitud del informante mediante reunión presencial, dentro del plazo de siete días hábiles desde la solicitud por los canales mencionados anteriores.

2. Presentada la información, se procederá a su Registro en el Sistema interno de gestión, garantizando los requisitos de confidencialidad previstos en la Ley 2/2023, y contenido en una base de datos segura y de acceso restringido al Responsable del Sistema y a los gestores a su cargo convenientemente designados al efecto, cumplimentando al menos la siguiente información:

- a) Fecha de recepción
- b) Código de identificación
- c) Fecha de admisión
- d) Actuaciones desarrolladas
- e) Medidas adoptadas
- f) Fecha de cierre

Todas las comunicaciones, nominativas o anónimas, quedarán debidamente registradas.

3. Recibida la comunicación, en un plazo de 7 días naturales siguientes a su recepción, se procederá a **acusar recibo** y a comunicar la justificación al informante, salvo que se pueda poner en peligro la confidencialidad de la comunicación.

4. Los datos personales relativos a las informaciones recibidas y a las investigaciones internas solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con la Ley 2/2023. En ningún caso podrán conservarse los datos por un período superior a diez años.

## 8.2 Fase de admisión

1. Registrada la comunicación, el Responsable del Sistema deberá comprobar si ésta se refiere a hechos o conductas que se encuentran dentro del ámbito material de aplicación definido en el artículo 2 de la Ley 2/2023, y si el informante se encuentra en el ámbito personal de aplicación definido en el artículo 3 apartados 1 y 2 de dicha Ley.

2. A tales efectos, el Responsable del Sistema, podrá requerir al informante la subsanación o la aportación de información adicional, en un plazo no superior a 7 días, informándole de las consecuencias de no cumplir el requerimiento.

3. Realizado el análisis sobre admisibilidad, el Responsable del Sistema decidirá en un plazo no superior a 10 días hábiles desde la fecha de entrada en el registro del sistema de gestión de información:

a) Inadmitir la comunicación de la información, lo supondrá la finalización del procedimiento, si concurre alguno de los siguientes casos:

i) Cuando el informante no se encuentre dentro del ámbito subjetivo de aplicación previsto en el artículo 3 de la Ley 2/2023, como son las reclamaciones de clientes que deberían realizarse a través del Servicio de Atención al Cliente.

ii) Cuando los hechos relatados carezcan de toda verosimilitud.

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

iv) Cuando la comunicación carezca manifiestamente de fundamento o existan, a juicio del Responsable del Sistema, indicios racionales de haberse obtenido mediante la comisión de un delito. En este último caso, además de la inadmisión, se remitirá al Ministerio Fiscal relación circunstanciada de los hechos que se estimen constitutivos de delito.

v) Cuando la comunicación no contenga información nueva y significativa sobre infracciones en comparación con una comunicación anterior respecto de la cual han concluido los correspondientes procedimientos, a menos que se den nuevas circunstancias de hecho o de Derecho que justifiquen un seguimiento distinto.

vi) Se basen en información pública.

vii) Estén relacionadas con disputas o conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación.

viii) Se fundamenten en meros rumores y/o no estén fundadas en sospechas o indicios concretos.

ix) Se basen en documentación que no se ha aportado y que no es accesible para la Entidad.

- x) Estén relacionadas con actuaciones o conductas que ya están siendo investigadas por la autoridad competente (policía, justicia, etc.).

La inadmisión será comunicada al informante dentro del plazo de 5 días hábiles siguientes a la adopción, salvo que la información fuera anónima.

- b) Admitir a trámite la comunicación.

La admisión a trámite se comunicará al informante dentro de los 5 días hábiles siguientes a su adopción, salvo que la comunicación fuera anónima.

- c) Remitir con carácter inmediato la información al Ministerio Fiscal cuando los hechos pudieran ser indiciariamente constitutivos de delito, o a la Fiscalía Europea en el caso de que los hechos afecten a los intereses financieros de la Unión Europea. En este supuesto, se producirá la finalización del procedimiento haciendo constar en el mismo esta circunstancia.

### 8.3 Fase de investigación o instrucción

1. La instrucción comprenderá todas aquellas actuaciones encaminadas a comprobar la verosimilitud de los hechos relatados.

2. El gestor delegado que designe el Responsable del Sistema se considerará instructor del procedimiento sin perjuicio de que, según la naturaleza de los hechos o conductas objeto de la comunicación, puedan intervenir otras áreas o departamentos especializados (Staff de Asesoría Jurídica, Staff de Recursos Humanos o consultores jurídicos externos) **sin facilitar en ningún caso la identidad del informante.**

3. El proceso de investigación quedará debidamente documentado, detallando los antecedentes, el objetivo, el alcance y las conclusiones alcanzadas en el sistema de gestión de informaciones.

4. Si durante la instrucción del procedimiento el gestor delegado apreciase que los hechos pudieran revestir el carácter de delito, el Responsable del Sistema remitirá las actuaciones al Ministerio Fiscal y emitirá un informe en el que se recoja expresamente esta circunstancia y la finalización del procedimiento.

5. En el plazo máximo de 15 días desde la resolución de admisión, se dará conocimiento a la persona afectada de la existencia de las actuaciones, de los hechos relatados de manera sucinta, salvo que dicha comunicación pueda facilitar la ocultación, destrucción y alteración de pruebas, en cuyo caso, el gestor delegado, de forma motivada, podrá modificar dicho plazo hasta que desaparezcan dichas circunstancias. En todo caso, la comunicación a las personas afectadas incluirá:

- la recepción de la comunicación y la fecha,
- las conductas/hechos que se atribuyen,
- el equipo/persona responsable de su gestión,
- el tratamiento que se realizará de sus datos de carácter personal, y
- el derecho de presentar alegaciones por escrito y a aportar las pruebas que considere convenientes y a solicitar una entrevista con el Responsable del Sistema o el gestor delegado a ser informado sobre el tratamiento de sus datos personales, y a poder ser asistido por un abogado.

En ningún caso se comunicará a las personas afectadas la identidad del informante y se advertirá al afectado de las consecuencias de un quebrantamiento de las garantías de confidencialidad y anonimato de las actuaciones, que pueden constituir una infracción muy grave tipificada en el artículo 63.1. c) de la Ley 2/2023.

6. Las comunicaciones que se realizan con la persona afectada deberán documentarse en el sistema de gestión de la información y dejar constancia de su resultado, tanto si han sido recogidas, expidiéndose el correspondiente acuse de recibo, como si han sido rehusadas.

7. Si el Responsable del Sistema considera conveniente la realización de una entrevista, o esta ha sido solicitada por el afectado, procederá a realizar el señalamiento con indicación de lugar, fecha y hora y se lo comunicará a la persona afectada.

Los actos de comunicación y entrevistas que, en su caso procedan, se realizarán con la máxima discreción posible, con la finalidad de preservar el secreto de las actuaciones, preservando la identidad del informante, terceros y afectados, y, en todo caso, garantizando la confidencialidad de las informaciones.

La entrevista se documentará y se incorporará al sistema de gestión de la información.

8. En cualquier momento durante la tramitación del procedimiento, el afectado tendrá derecho a acceder al contenido del expediente, siempre que dicho acceso no facilite la ocultación, destrucción y alteración de pruebas, en cuyo caso el gestor delegado podrá diferir el acceso de forma motivada, hasta que desaparezcan dichas circunstancias. En cualquier caso, se adoptarán las medidas necesarias para que el acceso se produzca preservando la identidad del informante, quedando prohibida cualquier actuación tendente a identificar al informante o terceros.

En el caso de que se proceda al acceso al expediente quedará constancia de esta circunstancia en el sistema de gestión de la información, con indicación del contenido, fecha y hora.

#### 8.4 Fase de resolución o finalización

1. Concluidas las actuaciones, el Responsable del Sistema emitirá un informe donde resolverá sobre el cumplimiento/incumplimiento de la normativa respecto los hechos/conductas objeto de comunicación, y así se comunicará a las partes involucradas a la mayor celeridad posible.

2. Emitido el informe, el Responsable del Sistema podrá:

a) Archivar del expediente.

b) Remitirlo al Ministerio Fiscal si, pese a no apreciar inicialmente indicios de que los hechos pudieran revestir el carácter de delito, así resultase del curso de la instrucción. Si el delito afectase a los intereses financieros de la Unión Europea se remitirá a la Fiscalía Europea.

c) Trasladar todo lo actuado a las autoridades o departamentos competentes, si se considera acreditada la comisión de alguna infracción a las que se refiere el ámbito material de aplicación previsto en el artículo 2 de la Ley 2/2023.

d) La adopción de acuerdo e inicio a un procedimiento disciplinario. El Responsable del SII remitirá el expediente al Staff de Recursos Humanos, si la persona que ha cometido la infracción es una persona empleada de la Entidad, para que adopte las medidas oportunas; en el caso de ser un miembro de un órgano de gobierno el Responsable del SII remitirá el expediente al Staff de Secretaría y Obra Social.

3. El plazo para finalizar las actuaciones y dar respuesta al informante, en su caso, no podrá ser superior a 3 meses desde la entrada en registro del sistema de gestión de la información, salvo casos de especial complejidad que requerirán una ampliación del plazo que podrá extenderse hasta tres meses adicionales.

## 9. Protección de datos personales

El SII de la Entidad garantiza la confidencialidad y la protección de datos personales de las personas involucradas en las comunicaciones durante todo el proceso de gestión de las mismas.

Los tratamientos de datos personales que deriven de la aplicación de la Ley 2/2023 se regirán por lo dispuesto en el título VI de la misma y en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

El Consejo de Administración tendrá la condición de responsable del tratamiento de los Datos Personales conforme a lo dispuesto en la normativa sobre Protección de datos personales.

La identidad del informante solo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora, y estos casos estarán sujetos a las salvaguardas establecidas en la normativa aplicable.

No se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una información específica o, si se recopilan por accidente, se eliminarán sin dilación indebida.

Cuando se obtengan directamente de los interesados sus datos personales se les facilitará la información a que se refieren los artículos 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 11 de la Ley Orgánica 3/2018, de 5 de diciembre.

A los informantes se les informará, de forma expresa, de que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.

El acceso a los datos personales contenidos en el SII quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente a:

- a) El Responsable del Sistema, y a quien lo gestione directamente.

- b) El Jefe del Staff de Recursos Humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra una persona trabajadora.
- c) El Jefe del Staff de Asesoría Jurídica de la Entidad si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.
- d) Los encargados del tratamiento que eventualmente se designen.
- e) El delegado de protección de datos (DPD) de la Entidad.

Será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario en el ejercicio de sus funciones técnicas relacionadas con la administración del sistema, la adopción de medidas correctoras en la Entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones que han sido objeto de comunicación, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la Ley 2/2023.

Si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de los mismos.

Los datos personales que sean objeto de tratamiento podrán conservarse en el SII únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados. Si la comunicación no es admitida, se procederá a la supresión de los datos, salvo que la inadmisión se produjera por la falta de veracidad de la información facilitada y ello pudiera constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, se suprimirán los datos personales, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del SII. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

El personal empleado y terceros deberán ser informados acerca del tratamiento de datos personales en el marco del SII.

## 10. Medidas de protección al informante

Los informantes de comunicaciones admitidas tendrán **derecho a protección** siempre que concurran las circunstancias siguientes:

- i) Tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación, aun cuando no aporten pruebas concluyentes, y que la citada información entra dentro del alcance del SII, de acuerdo con el ámbito de aplicación de la Ley 2/2023.
- ii) La comunicación se haya realizado conforme a los requerimientos previstos en la Ley 2/2023 y recogidos en la Política del SII y defensa del informante y en el presente procedimiento.

También tendrán derecho a protección las personas que hayan comunicado información sobre acciones u omisiones potencialmente irregulares de forma anónima pero que posteriormente hayan sido identificadas.

De acuerdo con el artículo 36 de la Ley 2/2023, se prohíben expresamente los actos constitutivos de represalia<sup>2</sup>, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación en el ámbito de SII.

Los informantes no incurrirán en responsabilidad respecto de la adquisición o el acceso a la información que es comunicada o revelada públicamente, siempre que dicha adquisición o acceso no constituya un delito.

Así mismo, conforme al artículo 37 de la Ley 2/2023, los informantes de comunicaciones admitidas dentro del SII tendrán acceso a las **medidas de apoyo** allí previstas.

## 11. Control de versiones

A continuación, se detalla el control de las versiones:

<b>Versión</b>	<b>Fecha aprobación</b>	<b>Control</b>
1	01-12-2023	Versión inicial

---

<sup>2</sup> Se entiende por represalia cualesquiera actos u omisiones que estén prohibidos por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, solo por su condición de informantes, o por haber realizado una revelación pública. Entre otras, se consideran represalias a efectos de la Ley 2/2023: suspensión del contrato de trabajo, despido o extinción de la relación laboral, degradación o denegación de ascenso, terminación anticipada de contratos de bienes o servicios, daños económicos o reputacionales, acoso, intimidación, inclusión en listas negras, denegación de permisos o formación, discriminación o trato desfavorable o injusto.