

**ESTRATEGIA APLICABLE AL SISTEMA INTERNO DE INFORMACIÓN Y DEFENSA DEL INFORMANTE EN LA  
EMPRESA PÚBLICA SOCIEDAD DE SERVICIOS DEL PRINCIPADO DE ASTURIAS, S. A.**

**Mayo 2023**

**La presente Estrategia fue aprobada por parte del Consejo de Administración de la empresa pública Sociedad de Servicios del Principado de Asturias, S. A., en reunión celebrada con fecha 18 de mayo de 2023**

**INDICE**

<b>1</b>	<b>ÁMBITO OBJETIVO .....</b>	<b>4</b>
<b>2</b>	<b>ÁMBITO SUBJETIVO .....</b>	<b>4</b>
<b>3</b>	<b>PRINCIPIOS GENERALES DE APLICACIÓN AL SISTEMA INTERNO DE INFORMACIÓN Y DEFENSA DEL INFORMANTE .....</b>	<b>5</b>
<b>4</b>	<b>RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN .....</b>	<b>7</b>
<b>5</b>	<b>MEDIOS PARA LA PRESENTACIÓN DE LA INFORMACIÓN .....</b>	<b>7</b>
<b>6</b>	<b>FASES DEL PROCEDIMIENTO .....</b>	<b>8</b>
<b>7</b>	<b>ESTRUCTURA DEL PROCEDIMIENTO DE GESTIÓN DE LAS INFORMACIONES RECIBIDAS .....</b>	<b>9</b>
<b>8</b>	<b>PUBLICACIÓN DE LA INFORMACIÓN RELATIVA AL SISTEMA INTERNO DE INFORMACIÓN .....</b>	<b>10</b>
<b>9</b>	<b>PROTECCION DE DATOS DE CARÁCTER PERSONAL/PERFILES CON ACCESO AL CANAL INTERNO .....</b>	<b>11</b>

El Sistema interno de información de la empresa pública Sociedad de Servicios del Principado de Asturias, S. A. se articula con la finalidad de dar cumplimiento a 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, por la que se incorpora al Derecho español la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019.

El Sistema interno de información es un elemento esencial de compromiso corporativo con el cumplimiento normativo, y su finalidad es la evitación de riesgos y/o comportamientos sancionables, protegiendo adecuadamente a aquellas personas que comuniquen las irregularidades de las que, en su entorno laboral o profesional, tengan conocimiento.

El presente sistema habilita un canal de informaciones que permite, al que entra en contacto con la organización, revelar la información de que dispone y que pueda constituir un ilícito. Ese canal interno de información garantizará en todo caso la confidencialidad del informante siendo posible, asimismo, su anonimato, si así se hubiera solicitado por su parte.

Este canal interno de información es complementario al canal externo correspondiente a la Autoridad Independiente de Protección del Informante.

## 1 ÁMBITO OBJETIVO

A través del sistema de información se protege a las personas físicas que informen acerca de:

a) Cualesquiera acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea siempre que:

- Entren dentro del ámbito de aplicación de los actos de la Unión Europea enumerados en el anexo de la Directiva (UE) 2019/1937 del Parlamento Europeo 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.
- Afecten a los intereses financieros de la Unión Europea tal y como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE).
- Incidan en el mercado interior, tal y como se contempla en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión Europea en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades o con prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades.

b) Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave. En todo caso, se entenderán comprendidas todas aquellas infracciones penales o administrativas graves o muy graves que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.

## 2 ÁMBITO SUBJETIVO

El sistema de información se aplicará a los informantes que trabajen en el sector privado o público y que hayan obtenido información sobre infracciones en un contexto laboral o profesional, comprendiendo en todo caso:

- a) Las personas que tengan la condición de empleados públicos o trabajadores por cuenta ajena.
- b) Los autónomos.
- c) Los accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de la empresa, incluidos los miembros no ejecutivos.
- d) Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

### **3 PRINCIPIOS GENERALES DE APLICACIÓN AL SISTEMA INTERNO DE INFORMACIÓN Y DEFENSA DEL INFORMANTE**

➤ **Garantía de la confidencialidad del proceso de información y, en el caso de que así se solicite por parte del informante, garantía de anonimato.**

Se garantizará, en todo caso, que el canal interno cuente con medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado, impidiendo el acceso al personal no autorizado.

Igualmente existirá garantía de confidencialidad cuando la comunicación sea remitida por canales de información que no sean los establecidos o a miembros del personal no responsable de su tratamiento.

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.

➤ **Protección del informante.**

Se reconoce la indemnidad de los informantes de buena fe.

Las personas que comuniquen o revelen infracciones contempladas en esta estrategia tendrán derecho a protección siempre que concurran las circunstancias siguientes:

a) Tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación o revelación, aun cuando no aporten pruebas concluyentes, y que la citada información entre dentro del ámbito de aplicación de la Ley 2/2023.

b) La comunicación o revelación se haya realizado conforme a lo indicado en la presente Estrategia.

Las medidas de protección del informante también se aplicarán, en su caso, específicamente a los representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante.

Quedan expresamente excluidos de la protección indicada aquellas personas que comuniquen o revelen:

a) Informaciones contenidas en comunicaciones que hayan sido inadmitidas previamente, de manera justificada, por no estar amparadas por la presente Estrategia, ni por el contenido de la Ley 2/2023.

- b) Informaciones vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación o revelación.
- c) Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores.

La protección indicada tiene una serie de limitaciones:

- a) La protección no excluirá la aplicación de las normas relativas al proceso penal, incluyendo las diligencias de investigación.
- b) La protección prevista para las personas trabajadoras que informen sobre infracciones del Derecho laboral en materia de seguridad y salud en el trabajo, se entiende sin perjuicio de la establecida en su normativa específica.
- c) La protección prevista no será de aplicación a las informaciones que afecten a la información clasificada.
- d) Tampoco afectará a las obligaciones que resultan de la protección del secreto profesional de los profesionales de la medicina y de la abogacía, del deber de confidencialidad de las Fuerzas y Cuerpos de Seguridad en el ámbito de sus actuaciones, así como del secreto de las deliberaciones judiciales.

En el supuesto de información relativa a alguna de las infracciones a las que se refiere la parte II del anexo de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, resultará de aplicación la normativa específica sobre comunicación de infracciones en dichas materias.

➤ **Prohibición de represalias.**

Se prohíben expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación, en los términos contemplados en el artículo 36 de la Ley 2/2023.

➤ **Presunción de inocencia.**

Se respetará plenamente la presunción de inocencia y al honor de las personas afectadas.

➤ **Protección de datos personales.**

Se producirá el pleno respeto de las disposiciones sobre protección de datos personales, conforme a lo previsto en la presente Estrategia y conforme a lo dispuesto en el Título VI de la Ley 2/2023.

#### 4 RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN

El responsable del Sistema interno de información en SERPA es un órgano colegiado, formado por los siguientes integrantes:

- Rafael Martínez Fuentes.
- Asunción Mormeneo Val.
- Mónica Sánchez López.

Se abstendrán de participar en la gestión y tramitación de los procedimientos, los integrantes de este órgano colegiado que puedan estar incurso en conflictos de intereses por razón del asunto que haya sido puesto en su conocimiento.

Este órgano deberá desarrollar sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad u organismo, no podrá recibir instrucciones de ningún tipo en su ejercicio, y deberá disponer de todos los medios personales y materiales necesarios para llevarlas a cabo.

El Consejo de Administración de la empresa pública Sociedad de Servicios del Principado de Asturias es el competente para la designación del/los responsable/s de la gestión del Sistema Interno de Información, y de su destitución o cese. Su nombramiento será notificado a la Autoridad Independiente de Protección del Informante, A.A.I., u órgano autonómico equivalente, en los términos establecidos en la Ley 2/2023.

#### 5 MEDIOS PARA LA PRESENTACIÓN DE LA INFORMACIÓN

- Se realizará a través del Canal Interno de Información de SERPA, que permite la presentación de comunicaciones a través de un formulario electrónico al que se accede *on line* desde la página corporativa [www.serpasa.es](http://www.serpasa.es). Este formulario estará disponible 24 horas al día, todos los días del año, con excepciones de interrupción temporal del servicio por razones de mantenimiento técnico.
- Al hacer la comunicación, el informante podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones.
- Se permitirá la presentación de comunicaciones anónimas en el canal interno.
- A solicitud del informante, también podrá presentarse la comunicación correspondiente mediante una reunión presencial dentro del plazo máximo de siete días desde la solicitud cursada a tal efecto. En tal caso, se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos, conforme a lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
- En la comunicación se podrán aportar o adjuntar documentos y/o evidencias que el informante estime conveniente para acreditar los hechos informados.

- En el caso de que la comunicación sea remitida por canales de información que no sean los establecidos o a miembros del personal no responsable de su tratamiento, estos la remitirán de manera inmediata al responsable del Sistema, quedando obligados a observar estricta confidencialidad.

## 6 FASES DEL PROCEDIMIENTO

### ➤ Recepción de informaciones

Presentada la información, se procederá a su registro, indicándose la fecha de recepción y asignándose a la comunicación un código identificativo individualizado.

### ➤ Análisis

El responsable del sistema deberá comprobar si la comunicación expone hechos o conductas que se encuentran dentro del ámbito de aplicación recogido en la presente Estrategia.

Realizado este análisis, adoptará y comunicará al informante, en un plazo que no podrá ser superior a quince días hábiles desde la fecha de presentación de la información, una de las decisiones siguientes:

#### a) **Inadmitir la comunicación**, en alguno de los siguientes casos:

- Cuando los hechos relatados carezcan de toda verosimilitud.
- Cuando los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico.
- Cuando la comunicación carezca manifiestamente de fundamento o existan 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.
- 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. En tal caso, se informará motivadamente acerca de las circunstancias acaecidas.

La decisión de inadmisión se comunicará al informante, salvo que la comunicación fuera anónima o el informante hubiera renunciado expresamente a recibir comunicaciones.

b) **Admitir a trámite la comunicación.** La admisión a trámite se comunicará al informante, salvo que la comunicación fuera anónima o el informante hubiera renunciado expresamente a recibir comunicaciones.

➤ **Instrucción**

La instrucción comprenderá las actuaciones encaminadas a comprobar la verosimilitud de los hechos relatados.

En ningún caso se comunicará a los sujetos afectados la identidad del informante ni se dará acceso a la comunicación.

Durante la tramitación del expediente las personas afectadas por la comunicación tendrán derecho a la presunción de inocencia, al derecho de defensa, así como a la misma protección establecida para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento

Las personas afectadas tendrán derecho de acceso al expediente -sin acceder a información que pudiera identificar a la persona informante- y, en el caso de considerarse necesario, a la formulación de alegaciones.

➤ **Finalización**

Concluidas todas las actuaciones, el responsable del sistema emitirá un informe que contendrá al menos:

- a) Una exposición de los hechos relatados y la fecha de registro.
- b) Las actuaciones realizadas.
- c) Las conclusiones alcanzadas tras la instrucción, y decisiones/actuaciones adoptadas.

Se remitirá 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, o, en su caso, a la autoridad, entidad u organismo que se considere competente para su tramitación.

## **7 ESTRUCTURA DEL PROCEDIMIENTO DE GESTIÓN DE LAS INFORMACIONES RECIBIDAS**

- Presentada la comunicación correspondiente, se remitirá al informante un acuse de recibo en el plazo máximo de siete días naturales siguientes a su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.

- La presentación de una comunicación por el informante no le confiere, por si sola, la condición de interesado en el procedimiento que se inicie.
- El plazo máximo para dar respuesta a las actuaciones de investigación no podrá ser superior a tres meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante, a tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación.
- Se garantizará la posibilidad de mantener la comunicación con el informante y, si se considera necesario, de solicitar a la persona informante información adicional. Siempre que la comunicación no sea anónima.
- Las informaciones recibidas y las investigaciones internas a que hayan dado lugar se incluirán en un Libro Registro, garantizando, en todo caso, los requisitos legales de confidencialidad a los que se refiere la Ley 2/2023.

Los datos personales relativos a las informaciones recibidas y a las investigaciones internas a que se refiere el apartado anterior solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con la ley 2/2023.

Particularmente, los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.

Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda 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, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada.

En ningún caso podrán conservarse los datos por un período superior a diez años.

## **8 PUBLICACIÓN DE LA INFORMACIÓN RELATIVA AL SISTEMA INTERNO DE INFORMACIÓN**

SERPA proporcionará la información relativa al uso del canal interno de información de forma clara y fácilmente accesible a través de la página de inicio de su web corporativa, incluyendo, de manera detallada y específica, la información específica sobre el uso del canal interno de información implantado.

Por lo que se refiere al canal externo de información, que sea habilitado por la Autoridad Independiente de Protección del Informante, A.A.I., se procederá a la inclusión en la web de SERPA de los datos de contacto correspondientes, conforme a lo previsto en el título III de la Ley 2/2023, en particular, las direcciones electrónica y postal y los números de teléfono asociados a dicho canal.

## 9 PROTECCION DE DATOS DE CARÁCTER PERSONAL/PERFILES CON ACCESO AL CANAL INTERNO

Los tratamientos de datos personales que se lleven a cabo en el ámbito del sistema de información interno se registrarán por lo dispuesto 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, y en el Título VI de la Ley 2/2023.

**Licitud:** El tratamiento de datos personales se considera lícito en virtud de lo que disponen los artículos 6.1.c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 8 de la Ley Orgánica 3/2018, de 5 de diciembre, y 11 de la Ley Orgánica 7/2021, de 26 de mayo.

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

- a) El responsable del sistema y a quien lo gestione directamente.
- b) Personal de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.
- c) Los servicios jurídicos de la entidad u organismo, 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.

Será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

**Limitación de la finalidad y supresión:** En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones.

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 Estrategia.

Los datos que sean objeto de tratamiento podrán conservarse durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.

Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

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.