PROCEDIMIENTO PARA LA GESTIÓN DEL SISTEMA INTERNO DE INFORMACION DE LA AGENCIA ESPAÑOLA DE SUPERVISIÓN DE INTELIGENCIA ARTIFICIAL

I. OBJETO Y ÁMBITO DE APLICACIÓN

- **Objeto**: La implementación de un sistema integral de Ética Institucional en la Agencia requiere de un marco organizativo que permita que se planteen las oportunas denuncias o comunicaciones por incumplimientos de la normativa aplicable y para luchar de forma efectiva y eficiente contra la corrupción.

  Este procedimiento establece las directrices para la gestión del canal interno de información de la AESIA, asegurando la confidencialidad, la protección de datos, la prohibición de represalias y el cumplimiento 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.

  La finalidad del presente sistema de información interno es, sobre la base de cualquier comunicación o denuncia presentada por cualquier persona que sea empleada pública en la Agencia, detectar y tratar posibles infracciones penales o administrativas graves o muy graves, así como infracciones del Derecho de la Unión Europea, en el contexto laboral o profesional de la Agencia.

- **Ámbito Material**: Se recibirán informaciones sobre acciones u omisiones que puedan constituir:

  - Infracciones del Derecho de la UE según el anexo de la Directiva (UE) 2019/1937. Deben diferenciarse del Canal de denuncias que recoge el artículo 85 del Reglamento (UE) 2024/1689, de 13 de junio de 2024, para incumplimientos en materia de dicho Reglamento de IA.

  - Infracciones que afecten a los intereses financieros de la UE o incidan en el mercado interior.

  - Infracciones penales o administrativas graves o muy graves, especialmente las que impliquen quebranto económico para la Hacienda Pública y la Seguridad Social.

- **Ámbito Subjetivo**: El canal está abierto a:

  - Empleados públicos y personal laboral de la Agencia.

  - Autónomos, accionistas, personal directivo, contratistas, subcontratistas y proveedores que trabajen para o bajo la supervisión de la Agencia.

  - Exempleados, voluntarios, becarios y candidatos en procesos de selección.

- Representantes legales de los trabajadores y personas que asistan al informante.

- **Exclusiones**: No se admitirán informaciones sobre conflictos interpersonales que afecten únicamente al informante, rumores, información ya pública o hechos que no se incluyan en el ámbito material 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.

II. ÓRGANOS Y RESPONSABILIDADES

- **Responsable de la implantación del Sistema interno de información**: De conformidad con el artículo 5.1 de la Ley 2/2023, de 20 de febrero, el Consejo Rector de la AESIA es el responsable de la implantación del Sistema Interno de Información, previa consulta con la representación legal de los trabajadores, y tendrá la condición de responsable del tratamiento de los datos personales de conformidad con lo dispuesto en la normativa sobre protección de datos personales.

- **El/la Responsable del Sistema interno de información**:

    - **Designación**: Se designa como **Responsable del Sistema** a la persona titular de la División Jurídica y Relaciones Institucionales, dependiente de la Secretaría General de la Agencia. Esta División gestionará los instrumentos jurídicos y valorará los expedientes sancionadores que pudieran derivarse de la gestión del canal interno de información de la AESIA, asegurando la confidencialidad, la protección de datos, la prohibición de represalias y el cumplimiento de la Ley 2/2023.

    - **Independencia y Autonomía**: El Responsable del Sistema actuará con total independencia y autonomía, sin recibir instrucciones en el ejercicio de sus funciones, y deberá disponer de los medios necesarios para ello.

      Su nombramiento y cese se producirán por resolución de la Presidencia y serán notificados a la Autoridad Independiente de Protección del Informante (A.A.I.) en un plazo de 10 días hábiles.

III. FASES DEL PROCEDIMIENTO

El procedimiento se estructura en cuatro fases principales: Recepción, Admisión, Instrucción y Terminación.

FASE 1: RECEPCIÓN DE LA INFORMACIÓN

1. **Canales de Presentación**:
    - La Agencia habilitará un medio telemático para presentar informaciones o denuncias internas, permitiendo la comunicación anónima, tanto de forma verbal como escrita. Se deberá formular a través de un canal seguro en la web de la AESIA, garantizando la confidencialidad y el acceso restringido a las denuncias por el responsable del Sistema.
2. **Registro de la Información**:
    - Toda comunicación recibida se registrará en un **libro-registro electrónico no público**, asignándole un código de identificación y de acceso restringido.
    - Este registro contendrá, como mínimo: fecha de recepción, código de identificación, actuaciones desarrolladas, medidas adoptadas y fecha de cierre.
    - El acceso al registro estará restringido al responsable del Sistema y solo se facilitará a la autoridad judicial bajo petición razonada.
3. **Acuse de Recibo**:
    - Se enviará un acuse de recibo al informante en un plazo máximo de **siete días naturales** desde la recepción de la comunicación a **través de la dirección de correo electrónico** que el informante deberá identificar de forma expresa con la comunicación.
    - No se enviará si el informante ha renunciado a recibir notificaciones, la comunicación es anónima o si el envío pudiera comprometer la confidencialidad.

FASE 2: TRÁMITE DE ADMISIÓN

1. **Análisis Preliminar**: El Responsable del Sistema evaluará si los hechos comunicados entran en el ámbito de aplicación de la ley y del canal interno.

   En los casos de **denuncia de acoso sexual**, se aplicará el Protocolo de actuación frente al acoso sexual y al acoso por razón de sexo en el ámbito de

la Administración General del Estado y de sus organismos públicos, aprobado mediante Real Decreto 247/2024, de 8 de marzo.

En los casos de **denuncia de acoso laboral**, se aplicará el Protocolo de actuación frente al acoso laboral en la Administración General del Estado, aprobado mediante Resolución de 5 de mayo de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba y publica el Acuerdo de 6 de abril de 2011 de la Mesa General de Negociación de la Administración General del Estado.

2. **Decisión de Admisión**: En un plazo máximo de **diez días hábiles** desde la comunicación, el Responsable del Sistema adoptará una de las siguientes decisiones:

    - **Inadmitir la comunicación**: Si los hechos carecen de verosimilitud, no constituyen una infracción cubierta por la ley, carecen de fundamento, se obtuvieron mediante un delito o no aportan información nueva y significativa sobre un caso ya cerrado. La inadmisión se notificará de forma motivada al informante en un plazo máximo de **5 días naturales**, salvo que sea anónima o haya renunciado a recibir comunicaciones.

    - **Admitir a trámite la comunicación**: Se notificará al informante en un plazo máximo de **5 días naturales**, salvo que sea anónima o haya renunciado a recibir comunicaciones.

    - **Remitir al Ministerio Fiscal o a la Fiscalía Europea**: Si los hechos indiciariamente pudieran ser constitutivos de delito, la remisión se hará sin dilación por la persona que ostente la Dirección mediante escrito a la sede que corresponda por razón de la competencia material y territorial.

    - **Remitir a otra autoridad competente**: Si el asunto no es competencia de la Agencia, el Responsable del Sistema dirigirá la comunicación a la entidad que considere competente para la tramitación de la denuncia o comunicación formulada.

FASE 3: INSTRUCCIÓN

1. **Objeto de la Instrucción**: Una vez admitida la comunicación, el Responsable del Sistema iniciará, en calidad de instructor, las actuaciones de investigación necesarias para comprobar la verosimilitud de los hechos relatados.

2. **Asistencia al instructor**: Cuando la complejidad del asunto o el volumen de la prueba presentada así lo requiera (p.ej. volumen ingente de correos electrónicos u otra documentación o pericial a valorar), el responsable del

Sistema podrá designar a una persona empleada de la Agencia para que le asista en la gestión de las labores instructoras, siempre que conste por escrito el cumplimiento de sus deberes estrictos de confidencialidad y la aplicación de la normativa de protección de datos del expediente.

3. **Garantías de la Persona Afectada**:

    - **Información**: Se le informará de los hechos que se le atribuyen, con una sucinta exposición de la denuncia y de cada uno de los hechos que se le imputen y que pudieran determinar, en su caso, una responsabilidad penal o disciplinaria de la persona afectada.

      Adicionalmente, se le informará de su derecho a la presunción de inocencia, al honor y a la defensa.

      Esta comunicación puede posponerse al trámite de audiencia si su anticipación pudiera comprometer la investigación (p. ej. riesgo de destrucción de pruebas).

    - **Alegaciones**: Tendrá derecho a presentar en un plazo de **10 días hábiles** las alegaciones que estime pertinentes y a acceder al expediente, sin que en ningún caso se revele la identidad del informante.

      En los supuestos en los que la complejidad del asunto o el volumen de la documentación o de la prueba a gestionar así lo justifiquen, el Responsable del Sistema podrá acordar la ampliación del plazo hasta un máximo de **20 días hábiles**.

4. **Garantías del Informante**:

    - **Confidencialidad**: Su identidad será reservada en todo momento y no se revelará a la persona afectada ni a terceros no autorizados. Solo podrá ser comunicada a la autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación, previa notificación al informante (salvo que comprometa la investigación).

    - **Prohibición de represalias**: Están prohibidos y serán nulos de pleno derecho cualesquiera actos de represalia (despidos, degradaciones, trato desfavorable, etc.) que se adopten sobre el informante como consecuencia de la comunicación efectuada a través del buzón de denuncias internas.

      Ello se entiende sin perjuicio de las posibles responsabilidades civiles, penales o disciplinarias en que hubiera podido incurrir como

consecuencia de su actividad personal o profesional como empleado público, de conformidad con la legislación aplicable.

- **Medidas de apoyo**: Se le ofrecerá información, asesoramiento y asistencia efectiva para su protección personal en caso de que el responsable del Sistema lo considere necesario.

5. **Plazo de Investigación**: El plazo máximo para concluir las actuaciones de investigación será de **tres meses** desde la recepción de la comunicación. En casos de especial complejidad, podrá prorrogarse el responsable del Sistema por otros **tres meses** adicionales.

FASE 4: TERMINACIÓN DE LAS ACTUACIONES

1. **Elaboración del Informe de Conclusiones**:

   - Finalizada la instrucción, el Responsable del Sistema elaborará un informe final que contendrá: la exposición de los hechos, las actuaciones realizadas y las conclusiones alcanzadas, con una valoración de las pruebas e indicios.

   - En los supuestos en los que la complejidad de la materia lo exija, el Responsable podrá solicitar el asesoramiento externo de la Abogacía General del Estado, que se someterá a los mismos deberes de confidencialidad establecidos para el responsable del Sistema por escrito y con anterioridad a la recepción cualquier petición al respecto.

2. **Decisión Final**: Con base en el informe, la Dirección de la Agencia adoptará una de las siguientes decisiones:

   - **Archivo del expediente**: Si no se confirman los hechos o no son constitutivos de infracción alguna. Se notificará al informante, salvo que sea anónima o haya renunciado a recibir comunicaciones, y a la persona afectada.

   - **Remisión al Ministerio Fiscal o a la Fiscalía Europea**: Si durante la instrucción se aprecian indicios de delito la remisión se hará sin dilación, por escrito, a la sede que corresponda por razón de la competencia material y territorial.

   - **Traslado a la autoridad competente**: Si se determina que la competencia corresponde a otro organismo el Responsable del Sistema dirigirá la comunicación a la entidad que considere competente para tramitar la denuncia formulada.

- **Inicio de un procedimiento disciplinario o sancionador**: Se trasladará al órgano competente dentro de la Agencia para la adopción de las medidas correspondientes.

3. **Comunicación del Resultado**: Se comunicará por escrito el resultado final de la investigación al informante, salvo que haya renunciado a ello o la comunicación fuese anónima.

IV. PROTECCIÓN DE DATOS Y CONSERVACIÓN DE LOS EXPEDIENTES

- El tratamiento de datos personales se regirá por el **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016**, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- El acceso a los datos estará estrictamente limitado al personal autorizado (i.e. Responsable del Sistema, RR.HH. en caso de ser necesaria la adopción de medidas disciplinarias, los Servicios Jurídicos para la emisión de informes preceptivos, y el Delegado de Protección de Datos).

- Los datos se conservarán por el tiempo imprescindible. Las comunicaciones inadmitidas o que no den lugar a investigación se destruirán a los **tres meses**, pudiendo conservarse de forma anonimizada para dejar evidencia del funcionamiento del sistema. En ningún caso, los datos del registro podrán conservarse por un período superior a **diez años**.

V. ANEXOS

ANEXO I

FICHA INFORMATIVA SOBRE EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL	
SISTEMA INTERNO DE INFORMACIÓN	
OBJETO	Ficha de tratamiento de datos personales incorporados a actividad de tratamiento de la Agencia Española de Supervisión de Inteligencia Artificial (AESIA).
NORMATIVA	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
UNIDAD	Secretaría General de la Agencia Española de Supervisión de Inteligencia Artificial.
RESPONSABLE DEL TRATAMIENTO	El Consejo Rector de la AESIA.
ENCARGADO DEL TRATAMIENTO	En el caso de que se externalice la gestión del Sistema Interno de Información a través de los servicios de un tercero, existirá un encargado de tratamiento de acuerdo con lo previsto en el correspondiente documento de adhesión, convenio o en el Pliego de Cláusulas Administrativas Particulares (PCAP) del contrato.
DELEGADO DE PROTECCIÓN DE DATOS	División jurídica, de relaciones institucionales y asuntos generales de la Secretaría General de la AESIA (info@aesia.gob.es).
ACTIVIDAD DEL TRATAMIENTO	Gestión del Sistema Interno de Información de la AESIA.
FINES DEL TRATAMIENTO	Recepción, registro y tramitación de comunicaciones y denuncias sobre acciones u omisiones que puedan ser constitutivas de infracción, así como la realización de las actuaciones de investigación interna y de protección del informante necesarias de acuerdo con lo previsto en la normativa aplicable.
LEGITIMACIÓN DEL TRATAMIENTO	• **Artículo 6.1.c) del RGPD**: tratamiento necesario para el cumplimiento de una obligación legal. • **Art. 6.1.e) del RGPD**: tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
BASE JURÍDICA	• 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 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

	• Ley 28/2022, de 21 de diciembre, de fomento del ecosistema de las empresas emergentes; Disposición Adicional 7ª. Creación de la Agencia Española de Supervisión de Inteligencia Artificial. • Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial.
CATEGORÍA DE INTERESADOS	• Informantes: Personas que comunican la información. • Personas afectadas: Personas a las que se refieren los hechos comunicados en la información. • Terceros mencionados: Otras personas mencionadas en la comunicación (testigos, colaboradores, etc.). • Personal con acceso a la información: responsable del Sistema, personal de apoyo designado por el responsable del Sistema, etc.
CATEGORÍAS DE DATOS PERSONALES	• **Datos de identificación del informante** (si no es anónimo): Nombre, apellidos, DNI/NIE, datos de contacto (dirección postal, correo electrónico, teléfono). La identidad del informante será siempre reservada. • **Datos de identificación de la persona afectada y terceros**: Nombre, apellidos, DNI/NIE, cargo profesional, datos de contacto. • **Información contenida en la comunicación**: Detalles de los hechos, fechas, lugares, descripción de las conductas, pruebas aportadas (documentos, grabaciones, etc.), que pueden contener datos de cualquier naturaleza necesarios para la investigación. • **Datos de naturaleza penal o administrativa**: Información sobre la presunta comisión de infracciones penales o administrativas graves o muy graves.
DESTINATARIOS	• El responsable del Sistema y el personal autorizado que lo gestione directamente. • El responsable de Recursos Humanos (o el órgano competente en el caso de empleados públicos), únicamente si procede adoptar medidas disciplinarias. • Los servicios jurídicos (Abogacía del Estado a través de la persona coordinadora del convenio), si proceden medidas legales. • El delegado de Protección de Datos. • Comité de Evaluación de riesgos y Ética Institucional para el ejercicio de funciones de asesoramiento o consultivas del buzón ético. • Ministerio Fiscal o la Fiscalía Europea, cuando proceda • Otros destinatarios contemplados en norma con rango de ley.
TRANSFERENCIAS INTERNACIONALES DE DATOS	No previstas.
CONSERVACIÓN Y SUPRESIÓN DE DATOS	Los datos personales tratados se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se hubieran recabado, así como para para determinar las posibles responsabilidades que pudieran derivarse de la misma. Comunicaciones no investigadas: Si no se inician actuaciones de investigación, los datos deberán ser suprimidos en un plazo máximo de **tres meses** desde la recepción de la comunicación. Podrán conservarse

	de forma anonimizada para dejar evidencia del funcionamiento del sistema. No se aplicará la obligación de bloqueo del artículo 32 de la LOPDGDD. Comunicaciones investigadas: Los datos se conservarán en el libro-registro durante el tiempo necesario para cumplir con la ley, con un plazo máximo de **diez años** desde su introducción (Art. 26.2 Ley 2/2023). Datos no veraces o irrelevantes: Los datos que no sean pertinentes o que se acrediten como no veraces se suprimirán de forma inmediata.
MEDIDAS DE SEGURIDAD	Se implementarán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, conforme al artículo 32 del RGPD y el Esquema Nacional de Seguridad (ENS) aplicable al sector público (Disposición adicional primera.2 en relación con el art. 77.1.d) LOPDGDD). Garantía de confidencialidad: El acceso a la información y los datos estará estrictamente limitado al personal autorizado, sujeto a un deber de secreto profesional. Se implementará un control de acceso lógico y físico. Protección de la identidad del informante: Se adoptarán medidas específicas para que la identidad del informante no sea revelada, tanto en los sistemas de información como en toda la documentación del expediente (Art. 24 LOPDGDD). Seguridad de los canales: Los canales de comunicación (electrónicos, verbales) estarán diseñados de forma segura para impedir el acceso de personal no autorizado y garantizar la integridad de las comunicaciones. Pseudonimización y cifrado: Se valorará el uso de técnicas de pseudonimización y cifrado de datos para minimizar los riesgos. Registro de accesos: Se mantendrá un registro de los accesos al sistema para su auditoría. Bloqueo y supresión segura: Se establecerán procedimientos para el bloqueo de datos (cuando aplique) y la supresión segura de la información una vez finalizados los plazos de conservación.
DERECHOS DE LOS INTERESADOS	Cualquier persona tiene derecho a obtener información sobre los tratamientos de sus datos que se lleve a cabo por la AESIA. Los destinatarios del tratamiento tienen derecho al acceso, rectificación, supresión, limitación y oposición al tratamiento de los datos en los términos previstos en los artículos 15 a 23 del RGPD. Puede ejercer estos derechos ante el responsable del tratamiento o ante el Delegado de Protección de Datos de la AESIA a través de las siguientes direcciones: • info@aesia.gob.es • Agencia Española de Supervisión de Inteligencia Artificial (DIR3: EA0054627) • c/ Veeduría, 2, 15001, A Coruña Asimismo, tienen derecho a reclamar ante la Agencia Española de Protección de Datos (AEPD): www.aepd.es • C/ Jorge Juan 6, 28001, MADRID