SISTEMA INTERNO DE INFORMACIÓN

DE LA SOCIEDAD MERCANTIL ESTATAL DE GESTIÓN INMOBILIARIA DE PATRIMONIO, M.P.S.A. (SEGIPSA)

Elaborado por:	Órgano de Cumplimiento Penal
Aprobado por:	Consejo de Administración
Fecha de la primera aprobación:	31 de mayo de 2023
Fecha de revisión:	
Responsable de la revisión:	*Responsable del Sistema Interno de Información*

ÍNDICE DE CONTENIDOS

1 Introducción

El 21 de febrero de 2023 se publicó en el BOE 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 traspone 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*.

La principal finalidad de la Ley es otorgar una protección adecuada a las personas físicas que, a través de los procedimientos que dicha norma recoge, proporcionen información sobre acciones u omisiones a que se refiere su artículo 2.

De conformidad con lo dispuesto en el art. 13.1.g) de la Ley 2/2023, de 20 de febrero, la SOCIEDAD MERCANTIL ESTATAL DE GESTIÓN INMOBILIARIA DE PATRIMONIO, M.P.S.A. (en adelante, también "SEGIPSA") está obligada a disponer de un *Sistema Interno de Información* en los términos previstos en dicha norma.

El presente documento recoge la configuración del ***Sistema Interno de Información*** de SEGIPSA que, entre otras cuestiones, contempla:

- ✓ El canal interno de información,
- ✓ El Responsable del *Sistema Interno de Información y,*
- ✓ El Procedimiento de gestión de informaciones.

La implantación del *Sistema Interno de Información* de SEGIPSA se llevará a cabo:

- ➢ Previa consulta con la representación legal de las personas trabajadoras, en cumplimiento de lo dispuesto en el art. 5.1 de la citada Ley.
- ➢ En el plazo máximo de tres meses a partir de la entrada en vigor de la Ley, es decir, antes del 13 de junio de 2023, en aplicación de su disposición transitoria segunda.

2 Objeto

El objeto de este documento es determinar la forma de llevar a cabo la gestión y tramitación de informaciones o comunicaciones recibidas, al amparo de la *Política del Sistema Interno de Información* aprobada en SEGIPSA, en aplicación 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*, por la que se transpone la Directiva (UE) 2019/1937, de 23 de octubre de 2019, del Parlamento Europeo y del Consejo (también, Directiva "Whistleblowing").

3 Ámbitos de aplicación

3.1 Ámbito material

En aplicación de lo establecido en el artículo 5 de la Ley 2/2023, sobre el *Sistema Interno de Información*, se deberán poder "*integrar (en el mismo Sistema) los distintos canales internos de información que pudieran establecerse dentro de la entidad*".

Adaptando esta premisa a la situación concreta de SEGIPSA y, con objeto de facilitar el uso de los canales internos de información por parte de todos los interesados, se podrá informar (denunciar/comunicar), sobre las siguientes cuestiones:

1) Infracciones Penales: Las acciones u omisiones que puedan ser constitutivas de infracciones penales, se encuentran establecidas en el *"Manual de Prevención de Delitos (POC- 14) del Sistema General de Cumplimiento Penal"* (https://www.segipsa.es/es/informacion-corporativa/Compliance-Penal/).

2) Prevención de Blanqueo de Capitales y Financiación del Terrorismo: Las acciones u omisiones se encuentran establecidas en el *"Manual de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo"*. (file:///N:/segip_net/docs/InfoCorporativa/Manual%20PBC%20yFT%20Enero%202023%20(R).pdf).

3) Fondos Europeos (PRTR): Las acciones u omisiones que pueden ser constitutivas de infracciones del Derecho de la Unión Europea, se encuentran recogidas en el *Plan de Medidas Antifraude* aprobado por SEGIPSA (https://www.segipsa.es/es/informacion-corporativa/plan-de-medidas-antifraude-fondos-prtr/).

4) Conducta y Ética Empresarial: Las infracciones relativas a esta materia, se encuentran establecidas en el *Código de Conducta y Ética Empresarial*, (https://www.segipsa.es/es/informacion-corporativa/CodCondEticaEmp/).

5) *Protocolo de Actuación y Prevención del Acoso Laboral en SEGIPSA*, del Plan de Igualdad, (file:///N:/segip_net/docs/RRHH/PLAN%20DE%20IGUALDAD.pdf)

6) Protección de datos personales: Las infracciones relativas a la Protección de los Datos Personales se encuentran recogidas en la *Política Corporativa de Protección de Datos Personales y Privacidad* (file:///N:/segip_net/docs/InfoCorporativa/Pol%C3%ADtica_Protecci%C3%B3n_Datos_Corporativa.pdf)

3.2 Ámbito personal

El *Sistema Interno de Información* de SEGIPSA 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, de acuerdo con el artículo 3 de la Ley y, en todo caso a:

1) Todos los empleados de SEGIPSA, independientemente del tipo de contrato y el nivel jerárquico, sean o no empleados públicos, por tiempo indefinido o trabajadores temporales.
2) El accionista único o cualquier miembro del Órgano de Administración, de la dirección o de órganos de supervisión de SEGIPSA.
3) Todos los profesionales autónomos, proveedores, clientes, contratistas, subcontratistas o cualquier otro tercero con el que SEGIPSA mantenga o haya mantenido anteriormente cualquier relación comercial o profesional, con inclusión de todas las personas que trabajen para los mismos o bajo la supervisión o dirección de contratistas, subcontratistas y proveedores.
4) Además, cualquier persona que tenga una relación laboral ya finalizada, voluntarios, becarios, con independencia de que perciban o no una remuneración e incluso las personas participantes en procesos de selección de personal, siempre y cuando la información sobre la infracción se haya obtenido durante el proceso de selección o de negociación precontractual.
5) Representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante.
6) Y, por último, también podrán informar las personas físicas que asistan a los informantes en el proceso, personas físicas relacionadas con el informante (como compañeros de trabajo o familiares del informante), así como personas jurídicas que puedan estar relacionadas con el informante.

4 Marco Regulatorio en SEGIPSA

Para cumplir con los requerimientos establecidos en la normativa vigente y determinar la prevalencia de los diferentes documentos y procedimientos internos, se establece la siguiente jerarquía:

1º. Política del Sistema Interno de Información:
Establece los principios y valores generales que deben orientar la implantación de esta materia en SEGIPSA y rigen todo el Sistema.

2º. Sistema Interno de Información:
Documento a través del cual se establece el estándar mínimo de garantías y protección obligatoria que determina la forma de llevar a cabo la gestión y tramitación de informaciones o comunicaciones recibidas, que será de aplicación a todos los procedimientos de gestión específicos.

3º. Procedimientos específicos de tratamiento de informaciones:
Regulan, en función de la materia, la forma concreta para el tratamiento de comunicaciones, determinan el órgano o personas responsables para su conocimiento e investigación, en su caso.

5 Identificación e Integración de canales internos de información

SEGIPSA dispone, actualmente, de los siguientes canales internos, para atender comunicaciones/informaciones/denuncias sobre distintas materias:

1. Infracciones Penales: canaldedenuncias@segipsa.es
2. Prevención del Blanqueo de Capitales y Financiación del Terrorismo: prevencionblanqueo@segipsa.es
3. Plan de Medidas Antifraude: antifraude@segipsa.es
4. Protección de Datos: protecciondedatos@segipsa.es
5. Código de Conducta y Ética Empresarial, Código de Conducta de Proveedores y Protocolo de Actuación y Prevención del Acoso Laboral: canaldeetica@segipsa.es

En aplicación de lo dispuesto en el art. 5.d) de la Ley 2/2023, de 20 de febrero, el presente *Sistema Interno de Información* dispone la integración de los distintos canales internos relacionados anteriormente, **en uno solo**, con un único enlace, alojado en la página web de SEGIPSA, en la pestaña de Transparencia: "Buzón Ético".

La implantación de dicho *canal interno de información* tendrá lugar, una vez cumplidos los requisitos de aprobación del presente documento por el Consejo de Administración de SEGIPSA y su traslado a la representación legal de las personas trabajadoras, mediante la aplicación informática que SEGIPSA ha contratado. Dicha aplicación permitirá garantizar la plena trazabilidad, integridad y confidencialidad de las comunicaciones, así como el anonimato de los informantes/denunciantes, al disponer de las siguientes Certificaciones: ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 27701:2019, la Certificación de Conformidad con el Esquema Nacional de Seguridad Categoría ALTA, así como estándar de conformidad de seguridad en la nube c5.

6 Forma y condiciones de las comunicaciones

El artículo 7.2 de la Ley 2/2023, de 20 de febrero, dispone:

> *"2. El canal interno deberá permitir realizar comunicaciones por escrito o verbalmente, o de las dos formas. La información se podrá realizar bien por escrito, a través de correo postal o a través de cualquier medio electrónico habilitado al efecto, o verbalmente, por vía telefónica o a través de sistema de mensajería de voz. A solicitud del informante, también podrá presentarse mediante una reunión presencial dentro del plazo máximo de siete días.*
>
> *En su caso, se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo a lo que establece el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.*

Además, a quienes realicen la comunicación a través de canales internos se les informará, de forma clara y accesible, sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea."

Dado que la norma ha establecido la posibilidad de optar entre varios formatos de comunicación (por escrito, verbal, o ambos), para garantizar la plena seguridad jurídica, el presente *Sistema Interno de Información* establece, de forma preferente, que las comunicaciones sean escritas a través de la aplicación informática del *canal interno de información*, ya que aquélla contempla que la comunicación/información/denuncia pueda realizarse de forma anónima, con plenas garantías de confidencialidad, integridad y trazabilidad.

También se admitirá, de acuerdo con lo dispuesto en el artículo 7.2 párrafo primero que, a solicitud del informante, la comunicación se presente mediante una reunión presencial dentro del plazo máximo de siete días. Previo consentimiento del informante, el contenido de dicha reunión, se recogerá en un Acta, ofreciéndole la posibilidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

Las comunicaciones podrán presentarse: bien incluyendo el informante sus datos identificativos, bien de forma anónima.

El canal interno de información de SEGIPSA "Buzón Ético" ofrece, por las Certificaciones referidas anteriormente, plenas garantías de seguridad, integridad y confidencialidad, permitiendo al Responsable del *Sistema Interno de Información* mantener el control y trazabilidad de las comunicaciones.

Sin perjuicio del *Canal Interno de Información* de SEGIPSA, existe la posibilidad de realizar comunicaciones sobre las cuestiones tratadas en este documento, directamente a través de los canales externos habilitados actualmente por las Autoridades competentes.

Así, en materia Antifraude relacionada con los proyectos y operaciones financiadas, total o parcialmente, con cargo a los Fondos Europeos, se podrán poner dichos hechos en conocimiento del Servicio Nacional de Coordinación Antifraude por medios electrónicos a través del canal habilitado en el siguiente enlace:

https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/paginas/denan.aspx

En los casos relativos a materias relacionadas con Protección de Datos y Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, agotada la vía del canal interno, los interesados podrán dirigirse a las correspondientes Autoridades de Control (AEPD y SEPBLAC, respectivamente).

7 Responsable del *Sistema Interno de Información*

El *Responsable del Sistema Interno de Información*, debe ser designado por el Consejo de Administración de SEGIPSA, órgano responsable legalmente de la implantación del presente Sistema.

El Consejo de Administración será competente para el nombramiento, destitución o cese del Responsable del Sistema.

Por su parte, el *Responsable del Sistema* tiene atribuida la gestión diligente del *Sistema Interno de Información* y de tratamiento adecuado de las comunicaciones recibidas, en cumplimiento del Sistema.

Según la Ley 2/2023, de 20 febrero, (art. 8.4) el Responsable del Sistema "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 para llevarlas a cabo"*. En las *"entidades u organismos en que ya existiera una persona responsable de la función de cumplimiento normativo o de políticas de integridad, cualquiera que fuese su denominación, podrá ser esta la persona designada como Responsable del Sistema, siempre que cumpla los requisitos establecidos en esta Ley"* (art. 8.6).

Dicho nombramiento será comunicado, de conformidad con el artículo 8.3 de la referida Ley, a la Autoridad Independiente de Protección al Informante (A.A.I.), tan pronto se encuentre habilitado el cauce correspondiente.

El *Responsable del Sistema* podrá habilitar a un empleado de SEGIPSA, con carácter excepcional y por razones accidentales (ausencias por enfermedad, causas de fuerza mayor, vacaciones), a fin de que se haga cargo de la gestión del Sistema para que éste se encuentre atendido en todo momento.

8 Procedimiento de gestión de informaciones

8.1 Recepción de Informaciones

Las Comunicaciones de información recibidas por cualquiera de las formas establecidas en los puntos anteriores serán revisadas por el *Responsable del Sistema* y, en el plazo máximo de 7 días naturales desde su recepción, se remitirá al interesado el acuse de recibo de las mismas, salvo que, el propio informante solicite su no remisión expresamente o, que dicho acuse pudiera poner en peligro la confidencialidad de la comunicación.

Una vez realizada la comunicación a través del medio electrónico habilitado, o bien se haya introducido en dicho Sistema la transcripción completa en los casos de reuniones presenciales, se asignará automáticamente, un código de identificación.

La información quedará registrada en los medios electrónicos habilitados de forma segura y de acceso restringido, únicamente a las personas autorizadas en función de la materia objeto de la comunicación.

8.2 Trámite de Admisión y Decisión Preliminar

El Responsable del Sistema realizará un análisis preliminar de la información y comprobará, únicamente, las siguientes cuestiones:

1. Si la Información comunicada entra dentro del ámbito de aplicación del *Sistema Interno de Información.*

2. El *Responsable del Sistema*, en caso de verificar que la comunicación entra dentro del ámbito de aplicación, deberá realizar un "juicio de verosimilitud" preliminar con los documentos disponibles y determinar, en informe razonado, si existen o no indicios de verosimilitud en la información comunicada. El Responsable, en caso de considerarlo necesario, podrá solicitar al interesado informante cualquier información adicional que resulte de ayuda para emitir el "juicio de verosimilitud".

En el plazo máximo de 10 días hábiles desde el acuse de recibo de la información, deberá tomar alguna de las siguientes decisiones:

I. **<u>Inadmitir a trámite</u>** la comunicación por algunas de las siguientes causas:

a. Que, no se encuentra dentro del ámbito de aplicación del *Sistema Interno de Información* aprobado por SEGIPSA.
b. Que, los hechos carecen de verosimilitud o no son constitutivos de una infracción.
c. Que, la información carece de fundamento o no hay pruebas suficientes para justificar la veracidad de la comunicación.

En todos los casos, se deberá documentar la decisión en un Informe razonado y suficientemente justificado.

II. **<u>Admitir a trámite</u>** la comunicación:

En caso de encontrarse dentro del ámbito de aplicación del Sistema y/o hallarse indicios suficientes para considerar la verosimilitud de la información, dependiendo del contenido y materia de la comunicación (Ética, Penal, Blanqueo de Capitales y Financiación del Terrorismo, Antifraude, Protección de Datos o cualesquiera otras que se integren en el Sistema).

El *Responsable del Sistema* dará traslado de la comunicación a las personas que, en cada caso, resulten responsables según los distintos procedimientos de tramitación de informaciones específicos que se encuentren vigentes en SEGIPSA, con objeto de continuar con el proceso de investigación interna.

El *Responsable del Sistema* deberá documentar su decisión en Informe razonado y suficientemente justificado. Asimismo, notificará su decisión al informante, tanto en caso de inadmisión como de admisión a trámite, en el plazo máximo de 10 días hábiles desde el acuse de recibo de la información.

III. **<u>Remisión al Ministerio Fiscal o a la Fiscalía Europea</u>**.

Si el *Responsable del Sistema*, tras el "juicio de verosimilitud" preliminar, tuviera motivos razonables para pensar que los hechos comunicados pudieran ser indiciariamente constitutivos de delito o que afectasen a los intereses financieros de la Unión Europea, deberá remitir, con carácter inmediato dicha información al Ministerio Fiscal o a la Fiscalía Europea, según corresponda.

En estos supuestos, el procedimiento de gestión de la comunicación no continuaría su tramitación interna, quedando ésta suspendida a la espera de la correspondiente resolución del Ministerio Fiscal o la Fiscalía Europea y/o petición de colaboración de las autoridades competentes.

8.3 Fase de Investigación

Una vez admitida a trámite la información comunicada y, habiendo dado traslado de la misma a los órganos /personas responsables en función de la materia, se aplicarán los procedimientos de tramitación de informaciones específicos que contemplarán las siguientes fases, independientemente de su denominación:

- **Análisis preliminar de la información:** Primer análisis de los datos comunicados y decisión de continuar o no con la investigación, según lo que indique cada procedimiento.
- **Instrucción:** Se aplicará según lo establecido en cada procedimiento de tramitación de informaciones específico.
- **Resolución:** Se aplicará lo establecido en cada procedimiento de tramitación de informaciones. En todo caso, la resolución deberá ser remitida al Responsable del Sistema para su conocimiento y archivo en el plazo máximo de 3 meses, o de su prórroga, si procede justificadamente.

8.4 Plazo máximo de duración de investigaciones

El Órgano o personas responsables en función de la materia, conforme a los diferentes procedimientos de gestión específicos vigentes, deberán comunicar, al informante, la resolución que corresponda, de forma suficientemente motivada.

En todo caso, el plazo máximo para finalizar la investigación y comunicar la resolución al informante, será de 3 meses a contar desde la recepción de la comunicación.

Excepcionalmente, en los casos de especial complejidad y de manera suficientemente razonada y documentada por el correspondiente órgano instructor, se podrá ampliar el plazo máximo de la investigación durante tres meses más, hasta un total de seis meses.

8.5 Registro de informaciones

De conformidad con el artículo 26 de la Ley, SEGIPSA dispondrá de un libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar, en los términos establecidos en dicho precepto, garantizando, en todo caso, los requisitos de confidencialidad.

9 Protección a los informantes y personas afectadas

9.1 Condiciones

Las personas que comuniquen infracciones previstas en el *Sistema Interno de Información*, tendrán derecho a protección, siempre que se cumplan las siguientes condiciones:

- La persona informante haya tenido motivos razonables para pensar que la información es veraz en el momento de la comunicación y la información se encuentre dentro del ámbito de aplicación de este Sistema.

- Que la comunicación se lleve a cabo conforme a lo establecido en el presente Sistema.

No habrá responsabilidad de ningún tipo para los informantes, en relación a la comunicación que realicen, siempre que concurran las mencionadas condiciones, y la información que se comunica no se haya obtenido cometiendo un delito.

9.2 Exclusiones

Quedarán expresamente excluidas de la protección las personas que comuniquen o revelen:

- Informaciones contenidas en comunicaciones que hayan sido inadmitidas por algún canal interno de información o por alguna de las causas previstas en el artículo 18.2.a) de la Ley 2/2023, de 20 de febrero.
- 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.
- Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores.
- Informaciones que se refieran a acciones u omisiones no comprendidas en el ámbito de aplicación de este Sistema.

9.3 Medidas

Las personas que comuniquen o revelen infracciones tendrán derecho a las medidas de protección establecidas en los artículos 35 y 36 de la Ley 2/2023, de 20 de febrero.

El presente Sistema establece el principio de protección del informante, prohibiendo expresamente cualquier acto de represalia, amenaza de represalia o tentativa de represalia contra la persona informante.

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.

Tal y como contempla el artículo 36.3 de la Ley 2/2023, de 20 de febrero, *"a título enunciativo, se consideran represalias las que se adopten en forma de:*

a) *Suspensión del contrato de trabajo, despido o extinción de la relación laboral o estatutaria, incluyendo la no renovación o la terminación anticipada de un contrato de trabajo temporal una vez superado el período de prueba, o terminación anticipada o anulación de contratos de bienes o servicios, imposición de cualquier medida disciplinaria, degradación o denegación de ascensos y cualquier otra modificación sustancial de las condiciones de trabajo y la no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido; salvo que estas medidas se llevaran a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral o reguladora del estatuto del empleado público correspondiente, por circunstancias, hechos o infracciones acreditadas, y ajenas a la presentación de la comunicación.*

b) *Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.*

c) *Evaluación o referencias negativas respecto al desempeño laboral o profesional.*

d) *Inclusión en listas negras o difusión de información en un determinado ámbito sectorial, que dificulten o impidan el acceso al empleo o la contratación de obras o servicios.*

e) *Denegación o anulación de una licencia o permiso.*

f) *Denegación de formación.*

g) *Discriminación, o trato desfavorable o injusto."*

Asimismo, las personas afectadas tendrán derecho a la presunción de inocencia, el derecho de defensa y el derecho de acceso al expediente en los términos previstos en la Ley 2/2023, a la misma protección que los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

10 Protección de datos de carácter personal

Las operaciones de tratamiento de datos de carácter personal realizadas para el cumplimiento de las disposiciones 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* se regirán 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* y 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 tratamiento de datos personales, tanto en los supuestos de comunicación internos como en casos de comunicación a través de los canales externos habilitados, se entenderá 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 tratamiento de datos personales derivado de una revelación pública se presumirá amparado en lo dispuesto en los artículos 6.1.e) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 11 de la Ley Orgánica 7/2021, de 26 de mayo.

La persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante o de quien haya llevado a cabo la revelación pública (art. 31.2 de la Ley 2/2023, de 20 de febrero).

El tratamiento de las categorías especiales de datos personales por razones de un interés público esencial se podrá realizar conforme a lo previsto en el artículo 9.2.g) del Reglamento (UE) 2016/679.

Los datos tratados en relación con el *Sistema Interno de Información* no podrán ser utilizados para fines distintos de los mencionados anteriormente.

Se facilitará al informante, la información requerida en los artículos 13 y 14 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y en el artículo 11 de la Ley Orgánica 3/2018, de 5 de diciembre.

Además, SEGIPSA garantiza la integridad, confidencialidad y disponibilidad de los datos personales con la adopción de las medidas técnicas y organizativas adecuadas y, en concreto, las garantías proporcionadas por las Certificaciones mencionadas en el precedente epígrafe 5.

El acceso a los datos personales contenidos en el *Sistema Interno de Información* (art. 32.1) 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 responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador. En el caso de los empleados públicos, el órgano competente para la tramitación del mismo.

c) El responsable de 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.

e) El delegado de protección de datos.

Por otro lado, la identidad del informante sólo podrá ser comunicada (art. 33) a la autoridad judicial, al ministerio fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.

Responsable del tratamiento: Consejo de Administración de la SOCIEDAD MERCANTIL ESTATAL DE GESTIÓN INMOBILIARIA DE PATRIMONIO, M.P.S.A. (SEGIPSA), de conformidad con lo dispuesto en el artículo 5.1 de la Ley 2/2023, de 20 febrero. El domicilio social de SEGIPSA se encuentra en José Abascal n.º 4- 3ª planta-28003 Madrid.

Se pueden ejercer los derechos de acceso a los datos, y en su caso, su rectificación o supresión o la limitación del tratamiento, o a oponerse al tratamiento o a la portabilidad de los datos de acuerdo con lo establecido en el RGPD. Estos derechos podrá ejercerlos solicitándolos por escrito a SEGIPSA en su dirección postal o a la DPD de SEGIPSA a través del enlace “Buzón Ético”.

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, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

11 Procedimiento sancionador

Estarán sujetos al régimen sancionador establecido en la Ley 2/2023, de 20 de febrero, las personas físicas y jurídicas que realicen cualquiera de las actuaciones descritas como infracciones en su artículo 63, pudiendo llegar a ser sancionados, por parte de la *Autoridad Independiente de Protección del Informante* (A.A.I.), con las siguientes penas de multa:

- Personas físicas responsables de las infracciones: multas de entre 1.001 y 300.000 euros.
- SEGIPSA, como persona jurídica: multas de entre 100.000 y 1.000.000 euros.

La cuantía de las multas se corresponderá, de acuerdo con lo establecido en el artículo 65 de la Ley, según la calificación de la infracción como: leve, grave o muy grave.

El régimen sancionador se regirá por lo establecido en los artículos 60 a 68 de la Ley 2/2023, 20 de febrero.

12 Formación, Publicación y Difusión

SEGIPSA promoverá la formación y difusión del *Sistema Interno de Información,* así como la de la *Política del Sistema*, con el objetivo de fomentar el uso y la cultura de información y de la comunicación para prevenir y detectar amenazas al interés público.

Este documento y la *Política* serán objeto de publicación en la página web y en la INTRANET de SEGIPSA y comunicados a todos los empleados de la sociedad.

13 Aprobación y Revisión.

El *Sistema Interno de Información*, aprobado por el Consejo de Administración de SEGIPSA, será implantado, previa consulta con la representación legal de las personas trabajadoras. Lo dispuesto en el presente documento prevalecerá sobre cualquier discrepancia que pudiera advertirse en los procedimientos de gestión de informaciones de materias específicas.

La revisión del *Sistema Interno de Información* se realizará, por su Responsable, anualmente o cuando se modifiquen las circunstancias que obliguen a ello, por razón de actualizaciones normativas y/o incorporación de mejoras procedimentales. Las modificaciones que resulten de su revisión, serán propuestas al Consejo de Administración para su aprobación.