RESOLUCIÓN DE LA SUBSECRETARÍA PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA POR LA QUE SE APRUEBA EL SISTEMA INTERNO DE INFORMACIÓN DEL MINISTERIO, EN 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 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, publicada en el BOE número 44, de 21 de febrero, por la que se transpone 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, establece en su artículo 9 que el órgano de administración u órgano de gobierno de cada organismo obligado por la misma aprobará el procedimiento de gestión de aquellas informaciones que se reciban a través del canal interno de información del que deben disponer.

En el artículo 5.2.h de la Ley se establece la necesidad de implantación de un sistema interno de información para posibilitar que la ciudadanía pueda informar, con garantías de confidencialidad y anonimato, sobre las acciones u omisiones previstas en la Ley, que deberá contar entre otros requisitos, con un procedimiento de gestión, que será aprobado por el órgano de gobierno del Ministerio y con una persona responsable del sistema interno de información.

Dicho sistema debe contar necesariamente con un canal interno de información que posibilite la comunicación de las infracciones contempladas en el artículo 2 de la citada Ley.

La puesta en marcha de este Sistema Interno de información, se encuentra además alineada con las medidas preventivas establecidas en el Plan de Medidas Antifraude del Ministerio y con el despliegue del IV Plan de Gobierno Abierto 2020-2024, de 29 de octubre de 2020, que fijó el marco institucional para mejorar la calidad democrática y reforzar la confianza de la ciudadanía en las instituciones, a través de dos compromisos: (a) implantar Sistemas de Integridad Pública para fortalecer la prevención mediante códigos de conducta, líneas de actuación, programas de formación y mecanismos de rendición de cuentas y (b) protección a los denunciantes que informen sobre corrupción, fraudes o violaciones de las leyes.

El Real Decreto 210/2024, de 27 de febrero, por el que se establece la estructura orgánica básica del Ministerio para la Transformación Digital y de la Función Pública atribuye en su artículo 13.3 a la Subsecretaría del Ministerio la ejecución de los planes y programas de inspección de los servicios y la evaluación del funcionamiento. Una de las competencias comprendidas en la función inspectora, es la de promover actuaciones que favorezcan la integridad profesional y comportamientos éticos de los empleados públicos y de las organizaciones, así como garantizar el cumplimiento de la normativa vigente.

Por tanto, conforme a lo dispuesto en el artículo 63.1.d) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y a propuesta de la Subdirección General de Recursos Humanos e Inspección de Servicios, esta Subsecretaría

RESUELVE

Aprobar la Estrategia del sistema interno de información y el Procedimiento de gestión del canal interno de información del Ministerio para la Transformación Digital y de la Función Pública, que se incluyen como anexos a esta resolución.

LA SUBSECRETARIA PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
(Firmado electrónicamente)

Iria Álvarez Besteiro

ESTRATEGIA DEL SISTEMA INTERNO DE INFORMACIÓN DEL MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

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, publicada en el BOE número 4, de 21 de febrero (en adelante, la Ley), por la que se transpone 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, partiendo de que la colaboración ciudadana resulta imprescindible para la eficacia del Derecho, incorpora los dos objetivos principales de la Directiva, que son el de "*proteger a las personas que informen sobre vulneraciones del ordenamiento jurídico*" y establecer "*los aspectos mínimos que han de satisfacer los distintos cauces de información*".

La Ley, de aplicación a las entidades que integran el sector público, tiene por finalidad otorgar una protección adecuada frente a las represalias que puedan sufrir las personas físicas que informen sobre alguna de las acciones u omisiones recogidas en su artículo 2. También tiene como finalidad el fortalecimiento de las infraestructuras de integridad de las organizaciones y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público.

En la Ley se contempla la existencia de dos tipos de sistemas de información a los que la ciudadanía puede acudir, para informar con garantías de confidencialidad y anonimato:

a) Interno: que sirve de cauce preferente para informar sobre las acciones u omisiones previstas en la Ley, con el fin de que la información sobre prácticas irregulares se conozca cuanto antes por la propia organización, para corregirlas o reparar lo antes posible los daños, si bien será el informante el que valore qué cauce seguir, interno o externo, según las circunstancias y los riesgos de represalias que considere.

b) Externo: con el fin de ofrecer a la ciudadanía una comunicación con una autoridad pública especializada, a estos fines, la Autoridad Independiente de Protección del Informante (A.A.I.) o autoridades autonómicas competentes, que puede resultar una opción preferible para el informante si teme sufrir alguna represalia en su entorno.

La presente estrategia responde a la obligación que establece el artículo 5.2 h) de la Ley de contar con una política o estrategia que enuncie los principios generales en materia de sistemas internos de información y defensa del informante.

1.- FINALIDAD

El Sistema interno de información del Ministerio para la Transformación Digital y de la Función Pública extiende su alcance a las unidades del Ministerio. Los organismos adscritos al departamento podrán adherirse al Sistema departamental en tanto no aprueben su propio sistema.

El sistema tiene como finalidad servir de cauce preferente de recepción de la información, para que los posibles casos de fraude y otras irregularidades dentro del ámbito de aplicación de la Ley, y que afecten a las competencias del Ministerio, sean conocidos cuanto antes por sus responsables.

2.- ÁMBITO MATERIAL DE APLICACIÓN DEL SISTEMA INTERNO DE INFORMACIÓN

El Sistema interno de información del Ministerio para la Transformación Digital y de la Función Pública debe permitir la recepción de comunicaciones de información relativas a hechos dentro del ámbito de competencias del Ministerio, que pudieran suponer:

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

1.- Entren dentro del ámbito de aplicación de los actos de la Unión enumerados en el Anexo de la Directiva (UE) 2019/1937, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno.

A tal efecto, debe tenerse presente que la citada Directiva establece normas mínimas comunes para la protección de las personas que informen sobre las siguientes infracciones del Derecho de la Unión: Infracciones que entren dentro del ámbito de aplicación de los actos de la Unión enumerados en el anexo relativas a los ámbitos siguientes: i) contratación pública, ii) servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo, iii) seguridad de los productos y conformidad, iv) seguridad del transporte, v) protección del medio ambiente, vi) protección frente a las radiaciones y seguridad nuclear, vii) seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales, viii) salud pública, ix) protección de los consumidores, x) protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información.

2.- 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); o

3.- Incidan en el mercado interior, tal y como se contemplan en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión 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 a 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.

c) Infracciones del derecho laboral en materia de seguridad y salud en el trabajo de las que informen los trabajadores, sin perjuicio de lo establecido en su normativa específica.

Este Sistema no será de aplicación para la presentación de informaciones que afecten a la información clasificada, a procedimientos de contratación que contengan información clasificada o que hubieran sido declarados secretos o reservados (art. 2 de la Ley 2/2023, de 20 de febrero).

3.- ÁMBITO PERSONAL DE APLICACIÓN DEL SISTEMA INTERNO DE INFORMACIÓN

Serán objeto de recepción, tramitación y seguimiento las informaciones recibidas de los informantes que trabajen en el sector privado o público y que hayan obtenido información sobre infracciones en el contexto laboral o profesional del Ministerio para la Transformación Digital y de la Función Pública, 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 una empresa, incluidos los miembros no ejecutivos.

d) Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

e) Los informantes que comuniquen o revelen públicamente información sobre infracciones que hubiera sido obtenida en el marco de una relación laboral o estatutaria ya finalizada, voluntarios, becarios, trabajadores en periodos de formación -con independencia de que perciban o no una remuneración-, así como a aquéllos cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.

4.- PRINCIPIOS GENERALES DEL SISTEMA INTERNO DE INFORMACIÓN

Con el objetivo de que el sistema sea efectivo, el Ministerio velará por el cumplimiento de todos los requisitos establecidos en 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. Entre ellos, cabe destacar:

a) Permitir a todas las personas referidas en el apartado 3 comunicar información sobre las infracciones previstas en el apartado 2.

b) Garantizar la confidencialidad de la identidad del informante, así como de cualquier tercero mencionado en la comunicación y de las actuaciones que se desarrollen en la gestión y su tramitación, así como la protección de datos, impidiendo el acceso de personal no autorizado.

c) Permitir la presentación y posterior tramitación de comunicaciones, incluso con carácter anónimo, por escrito.

d) Garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva dentro del Ministerio, con el objetivo de que el primero en conocer la posible irregularidad sea el propio organismo.

e) Ser independiente y aparecer diferenciado respecto de los sistemas de información de otras entidades y organismos.

f) Contar con una persona responsable del sistema, en los términos previstos en el artículo 8 de la Ley 2/2023, de 20 de febrero.

g) Contar con una política o estrategia en materia de sistemas internos de información y defensa del informante.

h) Contar con un procedimiento de gestión de las informaciones recibidas, aprobado por el órgano de gobierno del Ministerio.

i) Establecer las garantías para la protección de los informantes conforme a la Ley 2/2023, de 20 de febrero.

5.- PRINCIPIOS GENERALES DE PROTECCIÓN DEL INFORMANTE

De acuerdo con el Título VII "Medidas de protección" de la Ley 2/2023, de 20 de febrero, el Sistema de información garantizará que las personas que informen sobre infracciones normativas y de lucha contra la corrupción gocen de las siguientes medidas de protección:

5.1.- Condiciones de protección

5.1.1. Las personas que comuniquen o revelen infracciones de las previstas en el apartado 2 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 entra dentro del ámbito de aplicación de la Ley.

b) La comunicación o revelación se haya realizado conforme a los requerimientos previstos en la Ley.

5.1.2. Quedan expresamente excluidos de la protección prevista en esta ley aquellas personas que comuniquen o revelen:

a) Informaciones contenidas en comunicaciones que hayan sido inadmitidas por algún canal interno de información o por la Autoridad Independiente.

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.

d) Informaciones que se refieran a acciones u omisiones no comprendidas en el apartado 2.

5.1.3. Las personas que hayan comunicado o revelado públicamente información sobre acciones u omisiones de forma anónima pero que posteriormente hayan sido identificadas y cumplan las condiciones previstas en la ley, tendrán derecho a la protección que la misma contiene.

5.1.4. Las personas que informen ante las instituciones, órganos u organismos pertinentes de la Unión Europea infracciones que entren en el ámbito de aplicación de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, tendrán derecho a protección con arreglo a lo dispuesto en la ley en las mismas condiciones que una persona que haya informado por canales externos.

5.1.5. Las medidas de protección del informante previstas en el título VII de la ley también se aplicarán, en su caso, a:

a) personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso,

b) personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante, y

c) personas jurídicas, para las que trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa. A estos efectos, se entiende que la participación en el capital o en los derechos de voto correspondientes a acciones o participaciones es significativa cuando, por su proporción, permite a la persona que la posea tener capacidad de influencia en la persona jurídica participada.

5.2.- Prohibición de represalias

5.2.1. 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 conforme a lo previsto en la ley.

5.2.2. Se entiende por represalia cualesquier acto u omisión que esté prohibido por la ley, o que, de forma directa o indirecta, suponga un trato desfavorable que sitúe a las personas que la sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, debido a su condición de informantes, o por haber realizado una revelación pública.

5.2.3. A los efectos de lo previsto en la ley, y 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) 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.

5.2.4. La persona que viera lesionados sus derechos por causa de su comunicación o revelación, una vez transcurrido el plazo de dos años, podrá solicitar la protección de la autoridad competente que, excepcionalmente y de forma justificada, podrá extender el período de protección, previa audiencia de las personas u órganos que pudieran verse afectados (art. 36.4 de la Ley).

5.2.5. Los actos administrativos que tengan por objeto impedir o dificultar la presentación de comunicaciones y revelaciones, así como los que constituyan represalia o causen discriminación tras la presentación de aquellas al amparo de la ley, serán nulos de pleno derecho y darán lugar, en su caso, a medidas correctoras disciplinarias o de responsabilidad, pudiendo incluir la correspondiente indemnización de daños y perjuicios al perjudicado.

5.3.- Medidas de protección frente a represalias.

5.3.1. No se considerará que las personas que comuniquen información sobre las acciones u omisiones recogidas en el apartado 2 o que hagan una revelación pública de conformidad con la ley 2/2023, hayan infringido ninguna restricción de revelación de información, y aquellas no incurrirán en responsabilidad de ningún tipo en relación con dicha comunicación o revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública de dicha información era necesaria para revelar una acción u omisión en virtud de dicha ley, todo ello sin perjuicio de lo dispuesto en las normas específicas de protección aplicables conforme a la normativa laboral. Esta medida no afectará a las responsabilidades de carácter penal.

Lo previsto en el párrafo anterior se extiende a la comunicación de informaciones realizadas por los representantes de las personas trabajadoras, aunque se encuentren sometidas a obligaciones legales de sigilo o de no revelar información reservada. Todo ello sin perjuicio de las normas específicas de protección aplicables conforme a la normativa laboral.

5.3.2. 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.

5.3.3. Cualquier otra posible responsabilidad de los informantes derivada de actos u omisiones que no estén relacionados con la comunicación o la revelación pública o que no sean necesarios para revelar una infracción en virtud de la ley será exigible conforme a la normativa aplicable.

5.3.4. En los procedimientos ante un órgano jurisdiccional u otra autoridad relativos a los perjuicios sufridos por los informantes, una vez que el informante haya demostrado razonablemente que ha comunicado o ha hecho una revelación pública de conformidad con la ley y que ha sufrido un perjuicio, se presumirá que el perjuicio se produjo como represalia por informar o por hacer una revelación pública. En tales casos, corresponderá a la persona que haya tomado la medida perjudicial probar que esa medida se basó en motivos debidamente justificados no vinculados a la comunicación o revelación pública.

5.3.5. En los procesos judiciales, incluidos los relativos a difamación, violación de derechos de autor, vulneración de secreto, infracción de las normas de protección de datos, revelación de secretos empresariales, o a solicitudes de indemnización basadas en el derecho laboral o estatutario, los informantes no incurrirán en responsabilidad de ningún tipo como consecuencia de comunicaciones o de revelaciones públicas protegidas por la misma. Dichas personas tendrán derecho a alegar en su descargo y en el marco de los referidos procesos judiciales, el haber comunicado o haber hecho una revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública era necesaria para poner de manifiesto una infracción en virtud de la ley 2/2023.

5.4.- Medidas para la protección de las personas afectadas.

Durante la tramitación del expediente las personas afectadas por la comunicación tendrán derecho a la presunción de inocencia, al derecho de defensa y al derecho de acceso al expediente en los términos previstos en la ley 2/2023, así como a la misma protección establecida para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

5.5.- Supuestos de exención y atenuación de la sanción.

5.5.1. Cuando una persona que hubiera participado en la comisión de la infracción administrativa objeto de la información sea la que informe de su existencia mediante la presentación de la información y siempre que la misma hubiera sido presentada con anterioridad a que hubiera sido notificada la incoación del procedimiento de investigación o sancionador, el órgano competente para resolver el procedimiento, mediante resolución motivada, podrá eximirle del cumplimiento de la sanción administrativa que le correspondiera siempre que resulten acreditados en el expediente los siguientes extremos:

a) Haber cesado en la comisión de la infracción en el momento de presentación de la comunicación o revelación e identificado, en su caso, al resto de las personas que hayan participado o favorecido aquella.

b) Haber cooperado plena, continua y diligentemente a lo largo de todo el procedimiento de investigación.

c) Haber facilitado información veraz y relevante, medios de prueba o datos significativos para la acreditación de los hechos investigados, sin que haya procedido a la destrucción de estos o a su ocultación, ni haya revelado a terceros, directa o indirectamente su contenido.

d) Haber procedido a la reparación del daño causado que le sea imputable.

5.5.2. Cuando estos requisitos no se cumplan en su totalidad, incluida la reparación parcial del daño, quedará a criterio de la autoridad competente, previa valoración del grado de contribución a la resolución del expediente, la posibilidad de atenuar la sanción que habría correspondido a la infracción cometida, siempre que el informante o autor de la revelación no haya sido sancionado anteriormente por hechos de la misma naturaleza que dieron origen al inicio del procedimiento.

5.5.3. La atenuación de la sanción podrá extenderse al resto de los participantes en la comisión de la infracción, en función del grado de colaboración activa en el esclarecimiento de los hechos, identificación de otros participantes y reparación o minoración del daño causado, apreciado por el órgano encargado de la resolución.

5.5.4. 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, excluye de lo dispuesto en este apartado a las infracciones establecidas en la Ley 15/2007, de 3 de julio, de Defensa de la Competencia.

5.6.- Medidas para la protección de los datos personales de las personas afectadas.

Los tratamientos de datos personales que deriven de la aplicación de la ley 2/2023 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, 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 sistema interno de información debe impedir el acceso no autorizado y 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. 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 salvaguardas establecidas en la normativa aplicable.

Si la información recibida contuviera datos personales sujetos a protección especial, se procederá a su inmediata supresión, salvo que el tratamiento sea necesario por razones de un interés público esencial

conforme a lo previsto en el artículo 9.2.g) del Reglamento (UE) 2016/679, según dispone el artículo 30.5 de la Ley 2/ 2023.

En todo caso, 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.

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.

6.- GARANTÍAS EN CASO DE GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN POR TERCERO EXTERNO

La gestión del sistema interno de información se podrá llevar a cabo en el propio Ministerio o acudiendo a un tercero externo, en los términos previstos en el artículo 6 de la Ley. A estos efectos, se considera gestión del sistema, la recepción de informaciones.

El tercero externo garantizará el respeto de la independencia, confidencialidad, protección de datos y el secreto de las comunicaciones y no supondrá el menoscabo de las garantías y requisitos que para la gestión del sistema de información interna establece la ley. Tampoco supondrá atribución de responsabilidad en persona distinta de la figura nombrada como responsable del sistema establecido en el artículo 8 de la Ley. Tendrá la consideración de encargado de tratamiento a efectos de la legislación sobre protección de datos personales. El tratamiento se regirá por el contrato o acto referido en el artículo 28.3 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

7.- DIFUSIÓN Y FORMACIÓN

La presente Estrategia debe ser difundida adecuadamente, a través de información pública y accesible a través de la página web del Ministerio, de forma que se asegure el conocimiento y su comprensión, tanto por los empleados públicos del Ministerio como por la ciudadanía.

Igualmente, se garantizará la difusión del procedimiento de tratamiento de la información del Sistema de información interno entre los empleados del departamento, así como sobre las garantías respecto a la confidencialidad de la identidad de las personas informantes, a través de los medios adecuados que ayuden a su mayor difusión y conocimiento. Se proporcionará formación a los empleados del Ministerio sobre los requisitos del funcionamiento del Sistema Interno de Información.

8.- ACTUALIZACIÓN, SEGUIMIENTO Y REVISIÓN

Como medida preventiva destinada a la detección de posibles incidencias y al objeto de introducir las mejoras necesarias, anualmente se revisará el funcionamiento del sistema de información interno. Si se considera preciso, se procederá a la actualización de la presente estrategia o del procedimiento de gestión.

PROCEDIMIENTO DE GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN DEL MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA

1.- FINALIDAD DEL SISTEMA INTERNO DE INFORMACIÓN

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, (BOE núm. 4 de 21/02/2023), (en adelante, la Ley), establece, en su artículo 13 que todas las entidades que integran el sector público estarán obligadas a disponer de un sistema interno de información en los términos establecidos en dicha ley.

El Sistema interno de información es el cauce preferente para informar sobre las acciones u omisiones previstas en el apartado 2 de la Estrategia, siempre que se pueda tratar de manera efectiva la infracción y si el informante considera que no hay riesgo de represalia.

El Sistema interno de información del Ministerio para la Transformación Digital y de la Función Pública extiende su alcance a las unidades del Ministerio. Los organismos adscritos al departamento podrán adherirse al Sistema departamental en tanto no aprueben su propio sistema.

El Sistema interno de información, deberá, conforme a lo establecido en la ley:

a) Permitir a todas las personas referidas en el apartado 3 de la Estrategia comunicar información sobre las infracciones previstas en su apartado 2.

b) Estar diseñado, establecido y gestionado de una forma segura, de modo que se garantice la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, y de las actuaciones que se desarrollen en la gestión y su tramitación, así como la protección de datos, impidiendo el acceso de personal no autorizado.

c) Permitir la presentación de comunicaciones por escrito o verbalmente, o de ambos modos.

d) Integrar los distintos canales internos de información que pudieran establecerse dentro de la entidad.

e) Garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la correspondiente entidad u organismo con el objetivo de que el primero en conocer la posible irregularidad sea la propia entidad u organismo.

f) Ser independientes y aparecer diferenciados respecto de los sistemas internos de información de otras entidades u organismos, sin perjuicio de lo establecido en los artículos 12 y 14 de la Ley.

g) Contar con un responsable del sistema en los términos previstos en el artículo 8 de la Ley.

h) Contar con una política o estrategia que enuncie los principios generales del Sistema interno de información y defensa del informante y que sea debidamente publicitada en el seno de la entidad u organismo.

i) Contar con un procedimiento de gestión de las informaciones recibidas.

j) Establecer las garantías para la protección de los informantes en el ámbito de la propia entidad u organismo, respetando, en todo caso, lo dispuesto en el artículo 9 de la Ley.

2.- ÁMBITO MATERIAL DE APLICACIÓN DEL SISTEMA INTERNO DE INFORMACIÓN

2.1. El Sistema interno de información del Ministerio para la Transformación Digital y de la Función Pública debe permitir la recepción de informaciones relativas a hechos que pudieran suponer, dentro del ámbito de competencias del Ministerio:

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

1.- Entren dentro del ámbito de aplicación de los actos de la Unión enumerados en el Anexo de la Directiva (UE) 2019/1937, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno.

A tal efecto, debe tenerse presente que la citada Directiva establece normas mínimas comunes para la protección de las personas que informen sobre las siguientes infracciones del Derecho de la Unión: Infracciones que entren dentro del ámbito de aplicación de los actos de la Unión enumerados en el anexo relativas a los ámbitos siguientes: i) contratación pública, ii) servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo, iii) seguridad de los productos y conformidad, iv) seguridad del transporte, v) protección del medio ambiente, vi) protección frente a las radiaciones y seguridad nuclear, vii) seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales, viii) salud pública, ix) protección de los consumidores, x) protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información.

2.- 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); o

3.- Incidan en el mercado interior, tal y como se contemplan en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión 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 a 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.

c) Infracciones del derecho laboral en materia de seguridad y salud en el trabajo de las que informen los trabajadores, sin perjuicio de lo establecido en su normativa específica.

2.2. Esta protección no excluirá la aplicación de las normas relativas al proceso penal, incluyendo las diligencias de investigación.

2.3. La protección prevista en la Ley 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.

2.4. La protección prevista en la Ley no es de aplicación a las informaciones que afecten a la información clasificada. 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.

2.5. No se aplicarán las previsiones de la Ley a las informaciones relativas a infracciones en la tramitación de procedimientos de contratación que contengan información clasificada o que hayan sido declarados secretos o reservados, o aquellos cuya ejecución deba ir acompañada de medidas de seguridad especiales conforme a la legislación vigente, o en los que lo exija la protección de intereses esenciales para la seguridad del Estado.

2.6. En el supuesto de información o revelación pública de 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.

3.- ÁMBITO PERSONAL DE APLICACIÓN DEL SISTEMA INTERNO DE INFORMACIÓN

3.1. Serán objeto de recepción, tramitación y seguimiento las informaciones recibidas de los informantes que trabajen en el sector privado o público y que hayan obtenido información sobre infracciones en el contexto laboral o profesional del Ministerio para la Transformación Digital y de la Función Pública, 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 una empresa, incluidos los miembros no ejecutivos.

d) Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

e) Los informantes que comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral o estatutaria ya finalizada, voluntarios, becarios, trabajadores en periodos de formación -con independencia de que perciban o no una remuneración-, así como a aquéllos cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.

3.2. En relación con este procedimiento de gestión de la información, el personal adscrito al Ministerio está obligado a guardar la estricta confidencialidad sobre:

a) La identidad del informante.
b) La identidad de las personas afectadas por la comunicación.
c) La identidad de cualesquiera otras personas mencionadas en la comunicación.
d) Cualquier tipo de información comunicada a través del Sistema interno de información.

4.- CANAL INTERNO DE INFORMACIÓN

4.1. El Ministerio para la Transformación Digital y de la Función Pública implanta, en cumplimiento de la Ley, un canal interno de información para posibilitar la presentación de información respecto de las infracciones previstas en el artículo 2 de la Ley (apartado 2 del procedimiento), que estará integrado dentro del Sistema interno de información y será gestionado por las personas designadas por la Subsecretaría.

El informante podrá elegir que su información sea presentada como anónima, o bien identificarse al presentar la comunicación, en cuyo caso el informante podrá indicar una dirección postal a efectos de recibir las notificaciones, o si lo prefiere, una dirección de correo electrónico.

4.2. Requisitos:

Con el objetivo de que el canal sea efectivo, el Ministerio velará por el cumplimiento de todos los requisitos establecidos en la Ley. Entre ellos cabe destacar:

4.2.1. Garantizar la confidencialidad de la identidad del informante, así como de cualquier tercero mencionado en la información y de las actuaciones que se desarrollen en la gestión y su tramitación, así como la protección de datos, impidiendo el acceso de personal no autorizado. Salvo cuando la persona que comunique la información solicite expresamente lo contrario, se guardará total confidencialidad respecto de su identidad, de forma que la misma no será revelada a persona alguna. A tal fin, en todas las comunicaciones, actuaciones de verificación o solicitudes de documentación que se lleven a cabo, se omitirán los datos relativos a la identidad de la persona que hubiera remitido la información, así como cualesquiera otros que pudieran conducir total o parcialmente a su identificación, y lo mismo se hará con los que se refieran a los datos correspondientes a cualquier tercero mencionado en la información suministrada.

Asimismo, cuando se tuvieran que trasladar las actuaciones a otros organismos para que tramiten los procedimientos que correspondan, será de aplicación lo dispuesto en el párrafo anterior respecto a la documentación que se remita a esos otros órganos, salvo cuando se trate de la Autoridad judicial, del Ministerio Fiscal o de la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora. En estos casos, con carácter previo a revelar su identidad, se remitirá al informante un escrito explicando los motivos de la revelación, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial.

4.2.2. Admitir la presentación y posterior tramitación de informaciones anónimas.

4.3. **Vías para la presentación de informaciones en el canal interno**

En el canal interno, la información se podrá comunicar por escrito, mediante correo postal o de manera telemática a través de la aplicación informática habilitada al efecto, a través de las siguientes vías:

4.3.1 Información comunicada por escrito, de manera telemática. - Ésta será la vía preferente para comunicar la información. A través de la aplicación informática disponible en la intranet del Ministerio**.**

4.3.2. Información comunicada por escrito, mediante correo postal.- Si excepcionalmente se optara por esta vía, la información junto con la documentación acreditativa de los hechos de la que disponga el informante, habrá de enviarse en sobre cerrado poniendo en el anverso "A la atención personal de la Inspección de Servicios.- Ministerio para la Transformación Digital y de la Función Pública.- C/ Poeta Joan Maragall, 41, Planta 12- 28020 Madrid. En este caso, por parte de la Inspección de Servicios, se comunicará a la persona que hubiera remitido la información, siempre que sea posible por el medio que ésta haya designado, que la comunicación ha sido recibida y que se le dará el tratamiento establecido en la Ley. El informante podrá, asimismo, a través del canal señalado, efectuar la solicitud para realizar comunicaciones de cualquiera de las formas y por cualquiera de los medios previstos en el artículo 7.2 de la Ley.

5.- CANALES EXTERNOS DE INFORMACIÓN

El canal de información interno es el cauce preferente para proporcionar informaciones en el ámbito de la Ley, referidas a infracciones que tengan relación con la actividad del Ministerio para la Transformación Digital y de la Función Pública. No obstante, se informa de que existen los siguientes **canales externos**, a disposición de la ciudadanía:

a) **Canal Externo de Información de la Autoridad Independiente de Protección del Informante (A.A.I**), regulado en el título III de la Ley 2/2023 de 20 de febrero. En fecha actual, la Autoridad Independiente de Protección del Informante (A.A.I.) aún no ha sido creada, contando el Gobierno con un año para la aprobación de su Estatuto a partir de la entrada en vigor de la Ley. En cuanto el Canal Externo de Información de aplicación en la A.G.E. esté creado, se informará sobre la forma de acceso en la página web de este Ministerio.

b) **Infofraude:** cualquier persona que tenga conocimiento de hechos que pudieran ser constitutivos de fraude o irregularidad en relación con proyectos u operaciones financiados total o parcialmente con cargo a fondos procedentes de la Unión Europea podrá poner dichos hechos en conocimiento del Servicio Nacional de Coordinación Antifraude (S.N.C.A.) a través del canal habilitado al efecto por dicho Servicio (Infofraude) en la dirección web:
https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/CA-UACI/SNCA/Paginas/ComunicacionSNCA.aspx

O bien dirigirse a **OLAF** (Oficina Europea de Lucha contra el Fraude):

https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_es

c) O ante la **Fiscalía Europea**, sobre la que se dispone de la información al respecto en el siguiente enlace: https://www.eppo.europa.eu/en/reporting-crime-eppo

d) En el caso de que se trate de una información sobre posibles prácticas anticompetitivas, podrán utilizarse los canales externos de comunicaciones de la Dirección de Competencia de la **Comisión Nacional de los Mercados y la Competencia,** cuya información al respecto se desarrolla en el siguiente enlace: https://edi.cnmc.es/buzones-anonimos/sica

6.- GESTION DEL SISTEMA INTERNO DE INFORMACIÓN

Se designa como "Responsable del Sistema", a los efectos de los artículos 8 y 9 de la Ley 2/2023, de 20 de febrero, a la Subdirección General de Recursos Humanos e Inspección de Servicios de este Ministerio

El canal interno de información será gestionado por la Inspección General de Servicios del Ministerio, que contará con el apoyo jurídico de la Abogacía del Estado del Departamento y de la Abogacía del Estado que asuma el asesoramiento jurídico en cada Secretaría de Estado, en función de la naturaleza de la información a tratar.

Si la información sobre infracciones recibida estuviera relacionada con la ejecución de los fondos de la UE, la Inspección General de Servicios recabará la colaboración del Comité Antifraude (CAF) del Ministerio.

7.- PROCEDIMIENTO DE GESTIÓN DE LAS INFORMACIONES

El procedimiento deberá seguir las siguientes fases:

7.1. Recepción de informaciones

La persona que decida comunicar una información sobre una posible infracción deberá facilitar la máxima información disponible sobre los hechos comunicados, debiendo incluir expresamente:

a) El tipo de vínculo que el informante mantiene con el Ministerio para la Transformación Digital y de la Función Pública, de acuerdo con el apartado 3.1 de este Procedimiento.

b) La fecha o fechas en que se hubieran cometido los hechos comunicados como infracciones (aunque sea por aproximación).

c) La/s persona/s que, en su caso, fueran presuntamente responsables de dicha infracción;

d) Una descripción completa y precisa de los hechos;

e) Documentos, datos y demás fuentes de prueba o información que, en su caso, pudieran permitir la investigación de los hechos.

Cuando la comunicación se realice a través del canal electrónico accesible a través de la intranet, se generará en el mismo un aviso de transmisión correcta de la información. Cuando los hechos se comuniquen en soporte papel, de acuerdo con lo previsto en el apartado 4.3.2, se procederá a acusar recibo de la comunicación en el plazo de siete días naturales siguientes a su recepción, siempre que sea posible y no se ponga en peligro la confidencialidad de la comunicación.

7.2. Análisis preliminar y su resultado

7.2.1. Registrada la información, el gestor encargado de su tramitación deberá comprobar si aquella expone hechos o conductas que se encuentran dentro del ámbito de aplicación recogido en el apartado 2 del presente protocolo.

7.2.2. Realizado este análisis preliminar, el gestor decidirá, en un plazo que no podrá ser superior a diez días hábiles desde la fecha de entrada en el registro de la información:

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

1º Cuando los hechos relatados carezcan de toda verosimilitud, su descripción sea excesivamente genérica e inconcreta, la información remitida sea escasa, o falten elementos de prueba que permitan realizar una verificación razonable de la misma y una determinación mínima del tratamiento que debe .darse a dichos hechos.
2º Cuando los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico incluido en el ámbito material de aplicación del apartado 2 de este protocolo.
3º Cuando la información carezca manifiestamente de fundamento o existan, a juicio del gestor, indicios racionales de haberse obtenido mediante la comisión de un delito. En este último caso, además de la inadmisión, se remitirá con carácter inmediato la información al Ministerio Fiscal.
4º Cuando la información no contenga datos nuevos y significativos sobre infracciones en comparación con una información anterior respecto de la cual hubieran concluido los correspondientes procedimientos, a menos que se den nuevas circunstancias de hecho o de Derecho que justifiquen un seguimiento distinto. En estos casos, el gestor comunicará el resultado al informante de manera motivada.
5º Cuando la tramitación de la información no sea competencia del Ministerio para la Transformación Digital y de la Función Pública.
6º Cuando la comunicación corresponda a otros trámites, servicios, o procedimientos administrativos.

La inadmisión se comunicará al informante dentro de los cinco días hábiles siguientes a su adopción, salvo que la información fuera anónima o el informante hubiera renunciado a recibir comunicaciones referentes a su gestión.

b) Admitir a trámite la comunicación. La admisión a trámite se comunicará al informante dentro de los cinco días hábiles siguientes a su adopción, salvo que la comunicación fuera anónima o el informante hubiera renunciado a recibir comunicaciones referentes a su gestión.

Cuando los hechos comunicados pudieran ser indiciariamente constitutivos de delito, se remitirá con carácter inmediato la información al Ministerio Fiscal o a la Fiscalía Europea en el caso de que los hechos afecten a los intereses financieros de la Unión Europea.

7.3. Investigación

7.3.1. Una vez admitida a trámite la comunicación de la información, procederá llevar a cabo todas aquellas actuaciones encaminadas a comprobar la verosimilitud de los hechos relatados, pudiendo para ello mantener comunicación con el informante y, si se considera necesario, solicitarle información adicional, utilizando para ello la vía de comunicación seleccionada por el informante.

7.3.2. Se garantizará que la persona afectada por la información tenga noticia de la misma, así como de los hechos relatados de manera sucinta. Adicionalmente, se le informará del derecho que tiene a ser oída y a presentar alegaciones junto con los documentos y justificaciones que estime pertinentes por escrito en un plazo de diez días hábiles desde que reciba la comunicación de la información, así como del tratamiento de sus datos personales.
Esta comunicación podrá llevarse a cabo en el trámite de audiencia, si se considerara que su realización con anterioridad pudiera facilitar la ocultación, alteración o destrucción de pruebas.

7.3.3. Sin perjuicio del derecho a formular alegaciones por escrito, la instrucción comprenderá, siempre que sea posible, una entrevista con la persona afectada en la que, siempre con absoluto respeto a la presunción de inocencia, se le invitará a exponer su versión de los hechos y a aportar aquellos medios de prueba que considere adecuados y pertinentes. A fin de garantizar su derecho de defensa, la persona señalada como presunta infractora tendrá acceso al expediente sin revelar información que pudiera identificar a la persona informante, pudiendo ser oída en cualquier momento, y se le advertirá de la posibilidad de comparecer asistida de abogado.

7.4. Terminación de las actuaciones

7.4.1. Concluidas todas las actuaciones indagatorias, el gestor de la información emitirá un informe que contendrá al menos:

a) Una exposición de los hechos relatados y la fecha de registro.

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

c) Las actuaciones realizadas con el fin de comprobar la verosimilitud de los hechos.

d) Las conclusiones alcanzadas en la investigación y la valoración de las diligencias y de los indicios que las sustentan.

7.4.2. Emitido el informe, el gestor de la información propondrá a la autoridad competente la adopción de alguna de las siguientes decisiones:

a) El archivo del expediente, que será notificado al informante y, en su caso, a la persona afectada. En estos supuestos, el informante tendrá derecho a la protección prevista en la Ley, salvo que, como consecuencia de las actuaciones llevadas a cabo en fase de investigación, se concluyera que la información, a la vista de la información recabada, debía haber sido inadmitida.

b) La remisión 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 investigación. Si el delito afectase a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

c) El traslado de todo lo actuado a la autoridad u organismo que se considere competente para su tramitación.

d) La adopción de acuerdo de inicio de un procedimiento sancionador.

7.4.3. El plazo para finalizar las actuaciones y dar respuesta al informante, en su caso, no podrá ser superior a tres meses a contar desde la recepción de la información o, si no se remitió acuse de recibo al informante, a tres meses a partir del vencimiento del plazo de siete días naturales después de efectuarse la información, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, éste podrá extenderse hasta un máximo de otros tres meses adicionales.

Cualquiera que sea la decisión, se comunicará al informante, salvo que hubiese renunciado a ello o que la comunicación hubiese sido anónima.

7.4.4. El informante, por el hecho de comunicar la existencia de una posible infracción penal o administrativa, no tiene la condición de interesado, sino de colaborador con la Administración. La presentación de una comunicación por el informante no le confiere, por sí sola, la condición de interesado. Las investigaciones que puedan llevarse a cabo se iniciarán siempre de oficio.

7.4.5. Las decisiones adoptadas por los órganos con funciones de comprobación o investigación en relación con las informaciones presentadas a través de este Sistema, no serán recurribles en vía administrativa ni en vía contencioso-administrativa. Ello sin perjuicio del recurso administrativo o contencioso administrativo que pudiera interponerse frente a la eventual resolución que ponga fin al procedimiento sancionador que pudiese incoarse a raíz de los hechos relatados.

8.- INFORMACIÓN SOBRE PROTECCIÓN DE DATOS PERSONALES

8.1. Los tratamientos de datos personales que se deriven de la aplicación de la Ley 2/2023 se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), 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.

8.2. Los datos de carácter personal facilitados por el informante y los obtenidos de los procedimientos de investigación interna, serán tratados por la persona responsable del tratamiento para ser incorporados al Sistema interno de información de protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción previsto en 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.
Este tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1 e) del RGPD).

8.3. Asimismo, tal y como recoge el artículo 32 de la Ley 2/2023 de 20 de febrero, podrán tener acceso a la información que se recopile a través del Canal Interno de información las personas autorizadas siguientes:

- La persona responsable del sistema y quien lo gestione directamente.
- La persona responsable de recursos humanos competente de la adopción de medidas disciplinarias contra un trabajador.
- La persona responsable de los servicios jurídicos, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.
- Las personas encargadas del tratamiento de los datos.
- La persona que ejerce como delegado/a de protección de datos.

8.4. La finalidad del tratamiento: es la protección a las personas que, en un contexto laboral o profesional, detecten posibles infracciones y las comuniquen mediante los mecanismos regulados en la citada norma legal.

8.5. La identidad del informante será en todo caso reservada, y no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros. 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.

8.6. Las revelaciones hechas en virtud de este apartado estarán sujetas a salvaguardas establecidas en la normativa aplicable. En estos casos, con carácter previo a revelar su identidad, se remitirá al informante un escrito explicando los motivos de la revelación, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial.

8.7. Los datos personales obtenidos de las informaciones recibidas y aquellos que tengan su origen en 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 finalidad para la que fueron recabados. En particular,

se tendrá en cuenta lo previsto en los apartados 3 y 4 del artículo 32 de la Ley 2/2023, de 20 de febrero. En ningún caso podrán conservarse los datos por un período superior a diez años.

8.8. El Ministerio para la Transformación Digital y de la Función Pública ha habilitado las medidas técnicas y organizativas necesarias que garantizan la preservación de la identidad de la persona informante, la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, tal y como se señala en el artículo 33.2 de la Ley 2/2023 de 20 de febrero, adaptadas a las diferentes vías de recepción de la información (telemática o por correo postal).

8.9. Se suprimirán los datos que no sean necesarios para el conocimiento de la investigación, o no se refieran a conductas que estén incluidas en el ámbito de aplicación de este procedimiento. Igualmente se suprimirán transcurridos tres meses los datos referentes a informaciones sobre las que no se inicien actuaciones, a contar desde la recepción de la comunicación.

8.10. Categoría de datos objeto de tratamiento: datos de identificación, de contacto, financieros, económicos y profesionales del informante, afectados y terceros investigados. También podrán ser objeto de tratamiento los datos sujetos a categorías especiales por razones de un interés público esencial, en los términos previstos en el art. 30.5 de la Ley 2/2023.

8.11. Origen de los datos: el informante, quien realice una revelación pública y entidad pública o privada que los aporte en el curso de la investigación para el esclarecimiento de los hechos informados.

8.12. Los derechos de acceso, rectificación y supresión de sus datos, de limitación y oposición a su tratamiento, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, cuando procedan, se pueden ejercitar ante el responsable del tratamiento. En el ámbito del Ministerio para la Transformación Digital y de la Función Pública: a través del buzón de correo dpd@digital.gob.es, o por escrito: "Delegado/a de Protección de Datos.- Ministerio para la Transformación Digital y de la Función Pública.- C/Poeta Joan Maragall 41, Planta 12-28020 Madrid".

8.13. Será responsable del tratamiento de los datos personales la Subsecretaría del Ministerio. La Inspección de Servicios será la encargada del tratamiento de los datos personales en cuanto a la recepción de las comunicaciones y la Secretaria General de Administración Digital (SGAD) de la Secretaría de Estado de Función Pública respecto al soporte tecnológico para el canal de presentación de informaciones por vía electrónica.
En su condición de encargados del tratamiento y conforme dispone el artículo 28.3 del Reglamento (UE) 2016/679, la Inspección de Servicios y la SGAD:

a) Tratarán los datos personales según las instrucciones del responsable del tratamiento.
b) Garantizarán que las personas autorizadas a tratar los datos personales tengan contraído compromiso de confidencialidad, guarden secreto profesional sobre los mismos y no los comuniquen a terceros, salvo en aquellos casos en que deba hacerse en estricto cumplimiento de la ley.
c) Asistirán al responsable del tratamiento, a través de medidas técnicas y organizativas apropiadas y siempre que sea posible, para que pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III del Reglamento (UE) 2016/679.

d) En caso de finalización del encargo de tratamiento, facilitarán la devolución de los datos al responsable del tratamiento, de acuerdo con las especificaciones técnicas que este establezca.
e) Pondrán a disposición del responsable del tratamiento toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el Reglamento (UE) 2016/679, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable del tratamiento o de otro auditor autorizado por aquél.