SOSMATIC ASISTENCIA TECNOLÓGICA

SOSMATIC, S.L.

PROTOCOLO DEL SISTEMA INTERNO DE INFORMACIÓN

Versión	Fecha	Afecta	Breve descripción del cambio
1ª	**29-01-2018**	**Creación**	

ÍNDICE

1. INTRODUCCIÓN

De conformidad con las exigencias recogidas 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 por la que se transpone la Directiva (UE) 2019/1937 del Parlamento Europeo (en adelante "Ley 2/2023") y en el Código Penal, art.31bis, **SOSMATIC, S.L.** (en adelante, "**SOSMATIC**") ha procedido a la creación de un Sistema Interno de Información.

La Ley 2/2023 establece en su art.10 que las empresas del sector privado que tengan contratados 50 o más trabajadores están obligadas a disponer de un Sistema Interno de Información, así como aquellas que, no teniendo dichas dimensiones, hayan implementado un Sistema Interno de Información. Asimismo, el Código Penal, en el marco de la implementación del Modelo de Prevención de delitos, en su art.31.bis.5. 4º, requiere que se imponga la obligación en las empresas de informar de riesgos e incumplimientos del Modelo de Prevención de Delitos (en lo sucesivo "MPD") a los Compliance Officers.

Por lo anterior, y dado que la entidad tiene como principal interés la creación de una cultura empresarial de cumplimiento a la legalidad, es por lo que se ha creado el Sistema Interno de Información y se desarrolla el presente Protocolo.

2. IDENTIFICACIÓN

2.1. OBJETO

Este documento tiene como objeto establecer el procedimiento de tramitación de las comunicaciones de infracciones que se reciban a través del Sistema Interno de Información, incluyendo las pautas de actuación que deben seguirse desde que se recibe la comunicación de infracción por el Responsable del Sistema Interno de Información o por el Gestor Externo, hasta que se da una resolución a la misma, previa tramitación e instrucción.

El Sistema Interno de Información se configura como uno de los controles claves establecidos en el MPD para la prevención, detección y conocimiento de quebrantos éticos, incumplimientos normativos o ilícitos penales, de forma que las pautas que se recogen en este Protocolo son de obligado cumplimiento para todas las personas relacionadas con la entidad.

La entidad otorgará todos los recursos necesarios al Responsable del Sistema Interno de Información y a la Comisión de Compliance para tramitar y resolver adecuadamente las comunicaciones de infracciones que lleguen a través del Sistema Interno de Información, dotándoles, además, de autoridad, autonomía y acceso suficiente a la información de la entidad para que cumpla con sus funciones.

Integración de otros canales

De conformidad con la normativa en lo relativo al canal único, el canal integra y permite, además, lo siguiente

a) Comunicaciones de violaciones de seguridad
b) Comunicaciones relativas a ejercicio de derechos en protección de datos
c) Comunicación de otras cuestiones relativas a códigos de conducta

Se entiende por vulneración de código de conducta:

a) Cualquier incumplimiento de la normativa interna de LA EMPRESA, de los valores, pautas de actuación o normas de conducta que se recogen en la misma.
b) Cualquier contingencia que pueda suponer un riesgo para la reputación de LA EMPRESA.

En este caso, en el supuesto de ejercicio de derechos, comunicación de violación de seguridad o vulneración de código de conducta, el canal no permite la anomización del comunicante.

2.2. ÁMBITO DE APLICACIÓN

Este Protocolo es de aplicación y obligado cumplimiento por parte de todos los miembros de la entidad y personas externas que tengan conocimiento de infracción (persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores). Se incluye dentro del concepto "miembro":

- Empleados de la entidad.
- Los accionistas, partícipes o el Administrador Único.
- Profesionales y colaboradores vinculados a la entidad respecto a los que este pueda ostentar, directa o indirectamente, el control.
- Personal en prácticas.
- Personal contratado por medio de ETT.

3. DEFINICIONES

3.1. Sistema Interno de Información: Canal establecido por parte de la entidad para la realización de comunicaciones de infracciones en el ámbito del mismo.

3.2. Canal Externo de Información de la Autoridad Independiente de Protección del Informante: Sistema de información gestionado por

parte de una autoridad estatal, así como autoridades autonómicas al que pueden acudir los empleados de la entidad.

3.3. Infracciones:

- Incumplimiento de normativa interna.
- Infracción penal: delitos establecidos en el código penal, como delitos de estafa, fraude a la Hacienda Pública o Seguridad Social, acoso sexual, daños informáticos, blanqueo de capitales o delitos contra la salud pública, entre otros.
- Infracciones administrativas graves o muy graves: infracciones administrativas tales como, la solicitud indebida de devoluciones, beneficios o incentivos fiscales, ejercicio de actividades profesionales sin la licencia de actividad pertinente, solicitud de subvenciones de forma fraudulenta o uso y creación de facturas, justificantes u otros documentos análogos falsos, entre otras. En todo caso, se entenderán comprendidas dentro de este ámbito, las infracciones administrativas que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.
- Cualquier vulneración de la ley.

3.4. Informante: Persona que comunica una infracción.

3.5. Persona investigada: Persona respecto a la que se interpone la comunicación de infracción y que como consecuencia de la investigación pude ser sancionada disciplinariamente o se le pueda atribuir responsabilidad penal o administrativa.

3.6. Persona afectada: Persona que sufre los actos de la persona investigada diferente al Informante.

3.7. Responsable del Sistema: Persona responsable del Sistema Interno de Información nombrada por el Administrador Único. En este caso, el Responsable del Sistema es D. David Casas Cartagena.

3.8. Responsable de la investigación: persona designada por los Compliance Officers para llevar a cabo la investigación de una comunicación de infracción.

3.9. Gestor externo: Abogados externos que gestionan el Sistema Interno de Información.

3.10. Autoridad independiente de Protección del Informante (A.A.I): Autoridad estatal y autoridades autonómicas encargada de gestionar el sistema externo de información y de tramitar las denuncias interpuestas en dicho sistema.

4. SISTEMA INTERNO DE INFORMACIÓN

4.1. COMUNICACIÓN DE UNA INFRACCIÓN

La comunicación de infracciones puede realizarse de forma escrita o de forma verbal:

4.1.1. Comunicación de infracciones de forma escrita:

4.1.1.1. Plataforma online: Se ha creado una plataforma para la comunicación de infracciones de forma segura y confidencial gestionada por un

gestor externo, UNIVER IURIS, S.L. (en adelante "UNIVER IURIS"). El link de acceso al Sistema Interno de Información es el que se indica a continuación:

https://canal.uneon.es/sosmatic/

A través del link indicado, los miembros de la entidad pueden acceder a un formulario a través del cual se puede interponer una comunicación de información nominativa o anónima.

Tras la interposición de la comunicación de información, se generará un número identificativo que permitirá al Informante, cuando lo estime oportuno, conocer el estado de tramitación de la comunicación de infracción realizada a través del apartado "Consulta Estado de Comunicación" que aparece en la plataforma.

Esta plataforma permite el envío de audios.

4.1.1.2 Correo postal: el informante puede realizar la información por escrito a través de correo postal a la atención del Responsable del Sistema Interno de Información al domicilio social de la entidad[1].

4.1.2. Comunicación de infracción de forma verbal:

4.1.2.1. En reunión presencial: a solicitud del informante (en los datos indicados con anterioridad), la información podrá presentarse mediante reunión presencial o telemática con el Responsable del Sistema Interno de Información o el Gestor Externo dentro del plazo de siete días desde la solicitud de

[1] C/ de la Llacuna, 161, 3ª planta, (08018) Barcelona.

la misma. La información mediante reunión presencial o telemática deberá ser grabada. En este sentido, el Responsable del Sistema y/o el Gestor Externo deberán advertir de este aspecto al informante y se le informará del tratamiento de sus datos de acuerdo a los establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

4.1.2.3 Información comunicada por otros medios: en el supuesto que de una información sea remitida por otros medios o canales no establecidos en este protocolo, o bien a miembros de la entidad no responsables de su tratamiento, deberán ser comunicadas por el receptor mediante el sistema interno de información de la entidad.

Todas estas comunicaciones fuera de la plataforma deberán ser informadas a UNEON para que deje constancia de la misma en la plataforma de gestión, medio único, securizado y centralizado de gestión de incidencias.

4.2. CONTENIDO DE LA COMUNICACIÓN DE INFRACCIÓN

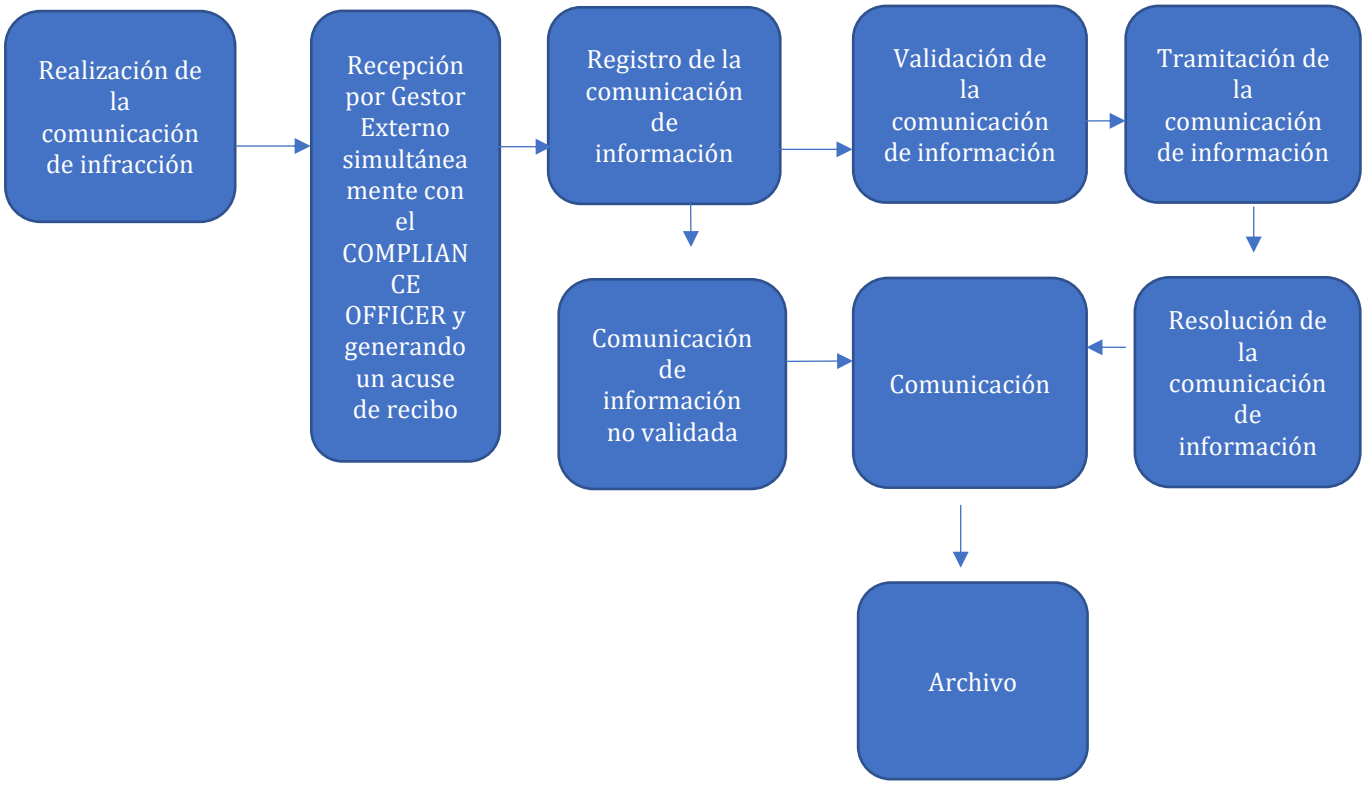
El contenido de la comunicación de infracción debe ser el siguiente:

- Identificación del informante (nombre completo, DNI, correo electrónico y vinculación con la entidad) una vez realizada la primera comunicación o marcar la opción anónimo.
- Identificación del departamento y/o actividad dónde se han producido los hechos o dónde se ha tenido conocimiento de los indicios referenciados.
- Nombre de la persona/s investigada o delimitación del área (si se conoce).
- Descripción de los hechos y circunstancias en las que ocurrieron.
- Todos los medios de prueba al alcance del informante que sean relevantes, oportunos y lícitos.
- Fecha en la que se produjeron los hechos.
- Personas que han presenciado o tienen conocimiento de los hechos.
- Cómo se ha tenido conocimiento del hecho comunicado.

Toda comunicación de información deberá ser interpuesta de buena fe.

El denunciante es responsable del contenido de la denuncia y como tal responderá de la veracidad de los hechos relatados, siendo advertido que se emprenderán las acciones legales pertinentes en caso que se demuestre la falsedad de los hechos relatados.

4.3. **PROCEDIMIENTO**



4.3.1. **Recepción de la comunicación de infracción**: UNIVER IURIS, como Gestor Externo, recibirá la comunicación de infracción simultáneamente con el compliance officer a través de la plataforma en la que quedan todas las actuaciones registradas, excepto en los casos que el denunciante haya marcado la

casilla de que denunciado es el compliance officer, por el que éste no recibirá comunicación alguna.

UNIVER IURIS tiene automatizado el acuse de recibo, antes del plazo de 7 días naturales siguientes a su recepción para remitir un acuse de recibo al informante, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.

4.3.2. **Registro de la comunicación de infracción:** UNIVER IURIS realizará el registro de la comunicación de infracción en la plataforma con todos los datos aportados por el informante.

4.3.3. **Comunicación de infracción válida:** En el caso de que la comunicación de la infracción se refiera a incumplimientos que se enmarcan en el ámbito objetivo del Canal (infracciones indicadas en el punto 3.3) la comunicación de infracción será validada.

4.3.4. **Comunicación de información no válida:** en el caso de que la comunicación de información se refiera a hechos que

- quedan fuera del ámbito objetivo de aplicación del canal (punto 3.3.) o que carezcan manifiestamente de fundamento: será comunicado al informante y se procederá al archivo de la comunicación de información,
- sean ajenos al ámbito objetivo del canal, pero relevantes para la entidad: serán remitidas al departamento correspondiente para el tratamiento de la incidencia, será comunicado al informante y se procederá al archivo de la comunicación de información.

4.3.5. **Tramitación de la comunicación de infracción:** la comunicación de infracción que haya sido previamente validada será tramitada. Ello significa que se comunicará a los miembros de la Comisión de Compliance, siempre que no exista con ellos incompatibilidad o un conflicto de intereses, y se nombrará al Responsable de la Investigación.

En este sentido, en coordinación con el Responsable del Sistema Interno de Información, la investigación interna podrá ser llevada a cabo por:

- uno o varios miembros de la Comisión de Compliance no afectados por la información.
- un miembro de la entidad que se considere competente en caso de que la información afecte directamente a todos los miembros de la Comisión de Compliance.
- un experto o asesor externo.
- un órgano compuesto por varias personas de la entidad con o sin un experto o asesor externo siempre que respecto a los mismos no exista incompatibilidad o un conflicto de intereses.

El Responsable de la Investigación llevará a cabo las actuaciones que considere necesarias de forma individual o en colaboración con las personas que considere necesario, siempre que sobre las mismas no existe incompatibilidad o conflicto de interés. Para ello podrá recabar toda la información y documentación que consideren necesaria de cualquier área, división o departamento, respetando siempre los derechos fundamentales de la/s persona/s que sean objeto de investigación. En caso de que se considere necesario, se podrá contar como complemento necesario e indispensable para salvaguardar la garantía de independencia con un asesor experto externo para la investigación y realización del dictamen.

En este sentido, durante la investigación, el responsable de la misma podrá mantener comunicación con el informante y, si lo considera necesario, solicitarle información adicional.

La duración máxima de las actuaciones de investigación será de tres meses desde la recepción de la comunicación de infracción hasta la resolución de la misma o, si no se remitió acuse de recibo al informante desde la finalización del plazo de siete días después de la comunicación. En casos de especial complejidad, que

deberán justificarse por escrito por parte del Responsable de la Investigación, podrá ampliarse el plazo por tres meses adicionales.

4.3.6. **Resolución de la comunicación de infracción:** Concluida la investigación, el Responsable de la Investigación realizará un informe que compartirá con la Comisión de Compliance para su aprobación. Este órgano, en coordinación con el Responsable del Sistema Interno de Información, tendrá poder de decisión para adoptar las medidas disciplinarias y correctivas pertinentes a imponer al trabajador o cualquier otra medida derivada del resultado de la investigación.

4.3.7. **Comunicación al Informante:** aprobado el Informe se comunicará al Informante que la tramitación de la comunicación de información ha concluido y que se procederá al archivo de la misma.

4.3.8. **Archivo**: tras la comunicación al Informante la comunicación de información será archivada.

Del todo el procedimiento constará un reflejo en la plataforma online a la que tendrá acceso el Informante que haya interpuesto una comunicación de información para poder consultar el estado de la tramitación de la misma (no su contenido). En el caso de que la comunicación de información se haya interpuesto por email, teléfono o de forma presencial las comunicaciones se realizarán por correo electrónico.

Lo anterior sucederá salvo en los casos en que el Informante indique que no quiere recibir información del procedimiento, supuestos en los que no se le remitirá comunicación alguna.

Todas las cuestiones deberán reflejarse en el canal como repositorio único de infracciones.

5. DERECHOS, PRINCIPIOS Y GARANTÍAS

5.1. DERECHOS DEL INFORMANTE

El informante tendrá derecho a:

- Decidir si desea realizar la comunicación de forma anónima o no anónima. En este último caso se garantiza la reserva de la identidad del informante.
- Formular la comunicación verbalmente o por escrito.
- Indicar un lugar donde recibir las comunicaciones: domicilio, correo electrónico, teléfono…
- Renunciar a su derecho a recibir comunicaciones.
- Comparecer ante el Responsable del Sistema Interno de Información o del Responsable de la Investigación si lo considera oportuno.
- Solicitar que la comparecencia sea realizada por videoconferencia u otros medios telemáticos que garanticen la identidad del informante y la seguridad y fidelidad de la comunicación.
- Ejercer los derechos que confiere la legislación en materia de protección de datos de carácter personal.
- Comunicar a través del Canal Externo de Información gestionado por parte de la Autoridad Independiente de Protección de Informante cualesquiera acciones u omisiones incluidas en el ámbito de ampliación de este protocolo y de la Ley 2/2023, ya sea directamente o previa comunicación a través del Sistema Interno de Información de la entidad.

5.2. PRINCIPIOS Y GARANTÍAS

Todos los miembros de la entidad tienen el derecho y la obligación de informar en el Sistema Interno de Información.

La disponibilidad de acceso al Sistema Interno de Información por parte de los miembros de la entidad como incentivo para el cumplimiento de su deber de comunicación de infracciones lleva aparejada la necesidad de proteger al informante.

Para ello, en la gestión y tramitación de informaciones, se aplicarán las siguientes garantías:

5.2.1. **Autonomía e Independencia del Responsable del Sistema:** el Responsable del Sistema, así como los demás miembros de la Comisión de Compliance tienen garantizada su autonomía mediante designación formal, por lo que se comprometen a velar por la confidencialidad y protección del informante sin admitir presiones ni injerencias de cualquier área que pudiera resultar implicada por la recepción de una comunicación de infracción.

5.2.2. **Confidencialidad y secretos de las comunicaciones**: Tratamiento confidencial que impida la revelación de datos de carácter personal, así como cualquier detalle que permitiera la identificación del informante por parte de las personas o departamentos relacionados con la comunicación, así como por cualquier profesional de la entidad que no sea miembro de la Comisión de Compliance. La identidad del informante

únicamente 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.

5.2.3. **Prohibición de Represalias**: La interposición de una comunicación de información realizada con buena fe, con independencia del acierto indagatorio o preventivo de la misma en términos de veracidad, no podrá generar represalia laboral alguna para el informante. Tampoco podrá generarse presión, en términos de acoso moral o psicológico, con el objetivo de influenciar en el cese de las acusaciones o como venganza por las mismas. Se trata de un compromiso asumido, mediante la aprobación de este Protocolo, por parte de los miembros de la Comisión de Compliance y el Administrador Único. Esta prohibición y la consiguiente protección del informante por posibles represalias regirá por un periodo de dos años tras la finalización de las diligencias de investigación internas.

De lo contrario, si la interposición de la comunicación es realizada con mala fe, SOSMATIC estará habilitado para ejercer las medidas disciplinarias que estime oportunas.

5.2.4. **Protección del Informante**: Los miembros de la Comisión de Compliance y, en especial, el Responsable del Sistema Interno de Información serán los encargados de velar por la protección del

informante, garantizando la no revelación de su identidad y datos personales, así como la ausencia de consecuencias negativas por la interposición de la comunicación de información. En caso de que se requiera al informante para la aportación de datos o testimonios adicionales de cara a observar la veracidad y gravedad de la comunicación realizada, habrá de hacerse garantizando que tanto en el requerimiento como en la respuesta se mantengan los niveles de protección antedichos.

5.2.5. **Ausencia de Conflictos de Intereses**: No formará parte de la tramitación e investigación de la comunicación ninguna de las personas relacionadas con la misma.

5.2.6. **Ausencia de Conflictos de intereses en la toma de decisiones del Administrador Único:** El Administrador Único se inhibirá de la toma de decisiones para la resolución de la comunicación de información si pudiera estar afectado por la misma.

5.3. CONFLICTO DE INTERESES

- Las comunicaciones de información serán remitidas por el Gestor Externo del Sistema Interno de Información al Responsable del Sistema Interno de Información, excepto cuando sea él el denunciado, que se gestionará con el sustituto.
- En los casos en que las comunicaciones de información afecten al

Responsable del Sistema Interno de Información, serán remitidas y tratadas con los miembros de la Comisión de Compliance, quedando el Responsable del Sistema al margen de toda investigación y propuesta de actuación.

- De afectar la comunicación de información al Responsable del Sistema y a parte de los miembros de la Comisión de Compliance, la misma será remitida por el Gestor Externo a los miembros no afectos de la Comisión de Compliance, personalizado en la responsable de RRHH de la compañía.
- En el caso de que la comunicación afecte a todos los miembros de la Comisión de Compliance, el Gestor Externo remitirá la comunicación de información al Responsable de CALIDAD, gestionándose con éste la investigación y propuesta de actuación.

5.4. **DERECHOS DE LAS PERSONAS INVESTIGADAS**

La persona investigada tiene derecho a la presunción de inocencia, derecho al honor, al derecho de defensa, de ser informado de las acciones u omisiones que se le atribuyen, debiendo tener acceso al expediente durante la tramitación del mismo y de ser oída en cualquier momento. La comunicación e información referida tendrán lugar en el tiempo y forma que el Responsable de la Investigación considere adecuado para garantizar el buen fin de la investigación.

Asimismo, las personas investigadas tendrán derecho a la misma protección establecida en este protocolo para los informantes en relación con la preservación de su identidad y la confidencialidad de los hechos y datos del procedimiento.

El acceso al expediente por parte de la persona investigada será en relación con los hechos que sean objeto de investigación, sin que sea posible un acceso que permita identificar la identidad del informante y de los terceros que se mencionen en la información suministrada. De modo que, en cada caso concreto, el Responsable

de la Investigación decidirá qué documentos e información es posible compartir con la persona investigada en caso de que lo solicite.

6. INFORME Y REGISTRO DE LA COMUNICACIÓN DE INFORMACIONES TRAMITADAS

De cada una de las comunicaciones de información se queda un registro en el Sistema Interno de Información numerado en el que se dejará constancia de la comunicación de información recibida, la fecha de recepción, su tramitación, archivo o supresión, el ámbito de afectación de la información, la investigación realizada, las acciones llevadas a cabo y las medidas de corrección implementadas. A la información indicada tendrá acceso únicamente el Responsable del Sistema Interno de Información y el Gestor Externo del Sistema Interno de Información.

La información indicada quedará almacenada de forma indefinida en el sistema con el objetivo de acreditar el funcionamiento del sistema ante una posible investigación judicial como elemento central del Modelo de Prevención de Delitos de la compañía.

7. TRATAMIENTO DE DATOS PERSONALES

El tratamiento de datos personales que deriven de la aplicación de esta política 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 y garantías de los derechos digitales, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales y en el TITULO VI 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 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.

Los interesados pueden ejercer los derechos recogidos en los art. 11 a 22 del Reglamento (UE) 2016/679. En concreto, los interesados podrán ejercitar su (i) derecho de acceso, (ii) derecho de rectificación, (iii) derecho de supresión, (iv) derecho de oposición, (v) derecho a la limitación, y, (vi) derecho a la portabilidad de sus datos mediante un escrito identificado con la referencia “Protección de Datos”, acompañando su DNI o documento equivalente, por las dos caras, dirigido al Responsable del Tratamiento de los datos.

No obstante, en caso de que la persona a la que se refieren los hechos relatados en la comunicación ejerciera el derecho de oposición se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales.

El acceso a los datos contenidos en el Sistema Interno de Información quedará limitado a:

- Gestor externo del Sistema Interno de Información, como encargado del tratamiento de los datos referidos.
- La entidad, como Responsable del Tratamiento de los datos. En este caso, la entidad habilitará el acceso a los datos contenidos en el Sistema Interno de Información al Responsable del Sistema, al Responsable de RRHH cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador o al Responsable legal si procede la adopción de medidas legales en relación con los hechos relatados en la comunicación.
- El Delegado de Protección de Datos, en su caso.

El tratamiento de datos tendrá el siguiente alcance:

- Registro de las comunicaciones recibidas a través de la plataforma online habilitada como Sistema Interno de Información.
- Conservación de los datos recibidos. El plazo de conservación de los datos será el estrictamente imprescindible para decidir sobre la procedencia de iniciar una investigación, siendo que no podrá exceder de tres meses, ni superar, en ningún caso, los diez años, de conformidad con lo dispuesto en el artículo 26.2 de la Ley 2/2023, de 20 de febrero.
- Supresión de los datos recibidos en los siguientes casos:
    - Transcurridos tres meses desde la recepción de la comunicación sin que se hubiese iniciado actuaciones de investigación, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema.

- Cuando los datos se refieran a conductas que no consistan ningún tipo de infracción.
- Cuando la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos.
- Si se acreditara que la información facilitada o parte de ella no es veraz.

Todos los datos serán tratados con la más estricta confidencialidad, únicamente por el personal autorizado para ello y con la única finalidad de investigar, tramitar y, en su caso, resolver la posible incidencia o irregularidad comunicadaen la medida en que sea necesario para la prestación de esos servicios. Sólo en el caso de que el hecho puesto en conocimiento de la empresa dé lugar a actuaciones administrativas o judiciales, los datos facilitados podrán ser comunicados a las autoridades competentes para su investigación y sanción.