



NICEPEOPLEATWORK, S.L.

SISTEMA INTERNO DE INFORMACIÓN



Versión	Fecha	Afecta	Breve descripción del cambio
1ª	13-09-2022	Creación	
2ª	24-01-2024	Actualización	Adaptación a la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción por la que se transpone la Directiva (UE) 2019/1937 del Parlamento Europeo.

Elaboración	Revisión	Aprobación
Cargo. APC	Cargo. Compliance Officer	Cargo. Órgano de Administración
Firma.	Firma.	Firma.
Fecha: 11-4-22	Fecha:	Fecha:

ÍNDICE

1. INTRODUCCIÓN	4
2. IDENTIFICACIÓN	5
2.1. OBJETO	5
2.2. ÁMBITO DE APLICACIÓN	5
3. DEFINICIONES	6
4. SISTEMA INTERNO DE INFORMACIÓN	8
4.1. COMUNICACIÓN DE UNA INFRACCIÓN	8
4.2. CONTENIDO DE LA COMUNICACIÓN DE INFRACCIÓN	10
4.3. PROCEDIMIENTO	11
5. DERECHOS, PRINCIPIOS Y GARANTÍAS	15
5.1. DERECHOS DEL INFORMANTE	15
5.2. PRINCIPIOS Y GARANTÍAS	16
5.3. CONFLICTO DE INTERÉS	18
5.4. DERECHOS DE LAS PERSONAS INVESTIGADAS	19
6. INFORME Y REGISTRO DE LA COMUNICACIÓN DE INFORMACIONES TRAMITADAS	20
7. TRATAMIENTO DE DATOS PERSONALES	21
8. AUTORIDAD INDEPENDIENTE DE PROTECCIÓN DEL INFORMANTE	23

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, NICEPEOPLEATWORK, S.L. (en adelante, “NPAW”) 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. 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 la entidad de informar de riesgos e incumplimientos del Modelo de Prevención de Delitos (en lo sucesivo, “MPD”) al Órgano de Control Interno o al Compliance Officer.

Por lo anterior, y dado que NPAW 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 Compliance Officer o 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 NPAW.

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

2.2. ÁMBITO DE APLICACIÓN

Este Protocolo es de aplicación y obligado cumplimiento por parte de todos los miembros de NPAW. Se incluye dentro del concepto “miembro”:

- Empleados de la entidad.
- Accionistas, partícipes o personas pertenecientes al Órgano de Administración.
- Profesionales y colaboradores vinculados a la entidad respecto a los que NPAW pueda ostentar, directa o indirectamente, el control.

- Personal en prácticas, voluntarios y trabajadores en periodos de formación, con independencia de que perciban o no una remuneración.
- Exempleados de NPAW, en relación con la información obtenida en el marco de la relación laboral ya finalizada.
- Personas cuya relación laboral con NPAW todavía no haya comenzado, en relación con la información obtenida durante el proceso de selección o de negociación precontractual.

3. DEFINICIONES

3.1. **Sistema Interno de Información:** Canal para la realización de comunicaciones de infracciones en el ámbito de la empresa.

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.
- Infracción administrativa grave o muy grave: pueden consistir, entre otras infracciones, en la solicitud indebida de beneficios, devoluciones o incentivos fiscales, el ejercicio de actividades profesionales sin la licencia de actividad pertinente, la solicitud de subvenciones de forma fraudulenta o el uso y creación de facturas, justificantes u otros documentos análogos falsos. 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 puede 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 Órgano de Administración. En este caso, NPAW ha designado a Dña. CAROLINA GOMEZ QUIÑO A como Responsable del Sistema.
- 3.8. **Responsable de la investigación:** persona designada por el Compliance Officer 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 encargadas de gestionar el Sistema Externo de Información y de tramitar las denuncias interpuestas en dicho sistema. En este sentido, la Ley 3/2023, de 16 de marzo, ha designado a la Oficina Antifraude de Cataluña como autoridad competente en esta comunidad autónoma.

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 despacho de abogados externo, Asesoría Penal Corporativa (en adelante “APC”). El link de acceso al Sistema Interno de Información es el que se indica a continuación:

<http://centinela.lefebvre.es/public/concept/1572431?access=%2bRltTh1y8KWIwiQMU5qXpbdgWIWrh2e4Oj3eGwqFtWU%3d>

A través del link indicado se accede 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 saldrá en pantalla un link que permitirá al informante, cuando lo estime oportuno, acceder de nuevo a la plataforma para conocer el estado de tramitación de la comunicación de infracción realizada.

4.1.1.2. **Correo electrónico:** El informante puede enviar un correo electrónico a la Responsable del Sistema Interno de Información (D^ª. Carolina Gómez -carolina.gomez@nicepeopleatwork.com-) o al Gestor Externo (proyectos@asesoriapenalcorporativa.es) para comunicar una infracción.

4.1.2. Comunicación de infracción de forma verbal:

4.1.2.1. **En reunión presencial o telemática:** a solicitud del informante (en los datos indicados con anterioridad) la información podrá presentarse mediante una reunión presencial o por medios telemáticos con la Responsable del Sistema Interno de Información, dentro del plazo de 7 días desde la solicitud de la misma.

Toda comunicación de una infracción de forma verbal mediante reunión presencial o telemática deberá documentarse de alguna de las maneras siguientes, previo consentimiento del informante:

- a) Mediante una grabación, en un formato seguro, duradero y accesible. En este supuesto, la Responsable del Sistema deberá advertir de este aspecto al informante, y se le informará del tratamiento de sus datos de acuerdo con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
- b) A través de una transcripción completa y exacta de la conversación. En este caso, sin perjuicio de los derechos que le correspondan al informante de acuerdo con la normativa sobre Protección de Datos, se le ofrecerá la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción realizada.

4.1.2.2. **Información comunicada por otros medios:** En el supuesto de que 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.

	PROTOCOLO DEL SISTEMA INTERNO DE INFORMACIÓN	V2_20240124
---	---	-------------

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 NPAW), si no se opta por realizar una comunicación de manera anónima.
- 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.
- Fecha en la que se produjeron los hechos.
- Todos los medios de prueba al alcance del informante que sean relevantes, oportunos y lícitos.
- 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.

4.3. PROCEDIMIENTO



4.1.1. **Recepción de la comunicación de infracción:** APC, como Gestor Externo, recibirá la comunicación de infracción a través de la plataforma en la que quedan todas las actuaciones registradas.

APC dispondrá 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.

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

4.1.3. **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.

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

- quedan fuera del ámbito objetivo y/o subjetivo 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 y/o subjetivo 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.

4.1.5. **Tramitación de la comunicación de infracción:** la comunicación de infracción que haya sido previamente validada será tramitada. Ello significa que se comunicará a la Responsable del Sistema Interno de Información, siempre que no exista incompatibilidad o un conflicto de intereses.

A su vez, la Responsable del Sistema remitirá las comunicaciones recibidas a los demás miembros del OCI, tras la referida verificación de ausencia de conflictos de intereses, y se nombrará al Responsable de la Investigación.

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

- la Responsable del Sistema Interno de Información,
- uno o varios miembros del Órgano de Control Interno, no afectados por la comunicación,
- un miembro de la entidad que se considere competente,

- 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 exista incompatibilidad o conflicto de interés. Para ello, podrá recabar toda la información y documentación que considere 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, de no haberse remitido 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.

4.1.6. Resolución de la comunicación de infracción: Concluida la investigación el Responsable de la Investigación realizará un informe que compartirá con la Responsable del Sistema para su aprobación (de no coincidir ambos cargos en la misma persona). Tras la emisión del informe por parte del

Responsable de la Investigación y su aprobación por la Responsable del Sistema, éste será compartido con el Órgano de Control Interno.

Este órgano 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.

4.1.7. **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.

4.1.8. **Archivo:** tras la comunicación al informante, la comunicación de información será archivada.

De 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 o de forma presencial, se procurará el registro documental de la comunicación por cualquier medio fidedigno, con el fin de que el informante cuente con evidencias suficientes de todo el procedimiento y pueda consultar el estado de la tramitación de la comunicación.

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.

En los reportes que se realicen al Órgano de Administración se incluirá información general relativa a la comunicación de información tramitada, omitiendo aquella información que permita la identificación del informante, es decir, se anonimizará la información en el reporte.

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 la 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 NPAW 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 de los Responsables del Sistema:** La Responsable del Sistema, así como los demás miembros del OCI, 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 los miembros del Órgano de Administración, ni de cualquier otra área que pudiera resultar implicada por la recepción de una comunicación de infracción.

5.2.2. **Confidencialidad:** 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 sean la Responsable del Sistema Interno de Información o miembros del OCI. 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 los miembros del OCI, la Responsable del Sistema y el Órgano de Administración. 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, NPAW estará habilitada para ejercer las medidas disciplinarias que estime oportunas.

5.2.4. **Protección del Informante:** Los miembros del OCI y, en especial, la Responsable del Sistema 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 interés en la toma de decisiones del Órgano de Administración:** Se inhibirán de la toma de decisiones para la resolución de la comunicación de información los miembros del Órgano de Administración que pudieran estar afectados por la misma.

5.3. CONFLICTO DE INTERÉS

- Las comunicaciones de información serán recibidas por el Gestor Externo del Sistema Interno de Información que, tras verificar la inexistencia de conflictos de intereses, las remitirá y compartirá con la Responsable del Sistema. A su vez, la Responsable del Sistema remitirá las comunicaciones recibidas a los demás miembros del OCI, tras la referida verificación de ausencia de conflictos de intereses.
- En los casos en que las comunicaciones de información afecten a la Responsable del Sistema, serán remitidas y tratadas con el Órgano de Control Interno, quedando la 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 del OCI, la misma será remitida por el Gestor Externo a los miembros no afectados del Órgano de Control Interno.
- En el caso de que la denuncia afecte a todos los miembros del OCI, el Gestor Externo remitirá la comunicación de información al Órgano de Administración gestionándose con este órgano la investigación y propuesta de actuación.
- Para el caso de que la comunicación de información afecte a todos los miembros del OCI y a algún miembro del Órgano de Administración, será remitida por el Gestor Externo a los miembros del Órgano de

Administración no afectados por la comunicación de información, y se gestionará con ellos la investigación y la propuesta de actuación.

5.4. DERECHOS DE LAS PERSONAS INVESTIGADAS

La persona investigada tiene derecho a la presunción de inocencia, al 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, preservándose su identidad y garantizándose 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 testigos que hayan participado en la investigación. De modo que, en cada caso concreto, la Responsable del Sistema de Información 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 la Responsable del Sistema Interno de Información, los miembros del Órgano de Control Interno, 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

Los tratamientos de datos personales que deriven de la aplicación de esta política se registrarán por lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos 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 del Proyecto de Ley 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, sin perjuicio de la aplicación de las pautas establecidas en el apartado 5.3. Además, podrá darse acceso a dichos datos 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.

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. No obstante, transcurridos tres meses desde la recepción de la comunicación sin que se hayan iniciado actuaciones de investigación, deberá procederse a la supresión de los datos recibidos, salvo que la

finalidad de la conservación sea dejar evidencia del funcionamiento del sistema.

- Supresión de los datos recibidos en los siguientes casos:
 - o 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.
 - o Cuando los datos se refieran a conductas que no consistan ningún tipo de infracción.
 - o Cuando la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos.
 - o 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 comunicada.