

POLÍTICA DEL SISTEMA INTERNO DE INFORMACIÓN



Fecha de aprobación y registro de cambios del documento

Versión	Fecha	Descripción
1.0.	20/06/2023	Aprobación del Consejo de Administración: actualización Canal Interno de Información (Ley 2/2023).
2.0.	21/09/2023	Modificación a petición de los representantes de los trabajadores.
3.0.	08/08/2024	Aprobación por parte del Consejo de Administración: actualización Fase 1 proceso certificador del Sistema de Gestión <i>Compliance</i> penal según UNE 19601:2017.
4.0.	25/09/2025	Aprobación por parte del Consejo de Administración: actualización del <i>Sistema de Gestión de Compliance penal</i> (cambios organizativos).

ÍNDICE

1. DEFINICIONES	4
2. OBJETIVO	7
3. ÁMBITO MATERIAL DE APLICACIÓN.....	8
4. ÁMBITO PERSONAL DE APLICACIÓN	10
5. OBLIGACIÓN DE REPORTAR INCUMPLIMIENTOS	11
6. COMPOSICIÓN DEL ÓRGANO RESPONSABLE DE LA GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN	12
7. VÍAS DE COMUNICACIÓN DEL SISTEMA INTERNO DE INFORMACIÓN.....	13
8. CANALES EXTERNOS DE INFORMACIÓN Y REVELACIÓN PÚBLICA 16	
9. PROTECCIÓN A LOS INFORMANTES.....	17
10. PROHIBICIÓN DE REPRESALIAS	19
11. MEDIDAS DE PROTECCIÓN FRENTE A REPRESALIAS	21
12. MEDIDAS DE PROTECCIÓN PARA LAS PERSONAS SOBRE LAS QUE VERSA LA COMUNICACIÓN	23
13. SANCIONES.....	24
14. CONFIDENCIALIDAD	25
15. PROTECCIÓN DE DATOS	27
16. PRINCIPIOS BÁSICOS DEL PROCEDIMIENTO GIR	30
17. REGISTRO DE COMUNICACIONES.....	31

1. DEFINICIONES

Se relacionan a continuación las definiciones de aquellos conceptos que se utilizarán de manera frecuente en el presente documento (citados en *cursiva*):

- **PERSÁN/la Organización/la Compañía:** incluye a la sociedad PERSÁN, S.A.
- **Oficina de Cumplimiento Normativo:** órgano interno de *PERSÁN* de carácter colegiado que está dotado de poderes autónomos de iniciativa y control, al que se le confía, entre otros cometidos, la responsabilidad de supervisar el funcionamiento y observancia del *Sistema de Gestión de Compliance penal* de la *Organización* tanto dentro como fuera del territorio nacional español. La existencia de este Órgano responde tanto a las exigencias establecidas en la normativa española (artículo 31 bis del Código Penal español), como a las mejores prácticas internacionales, en cuanto a la supervisión del *Sistema de Gestión de Compliance penal*.
- **Departamento de Risk&Compliance:** integrado por la *Oficina de Cumplimiento Normativo*, así como por las áreas de Gestión de Riesgos y Auditoría Interna. Tiene como función principal, además de las competencias establecidas para la *Oficina de Cumplimiento Normativo*, la supervisión de la integridad financiera y no financiera, la eficacia de los controles internos y la gestión de riesgos corporativos. El *Departamento de Risk&Compliance* estará liderado por el *Chief Risk & Compliance Officer*.
- **Consejo de Administración:** órgano que tiene la responsabilidad y autoridad fundamental de las actividades, la gobernabilidad y las políticas de *PERSÁN* y al que la *Alta dirección* informa y rinde cuentas.
- **Alta dirección / Comité de Dirección:** es el órgano de alto nivel dentro de *PERSÁN* que depende directamente del *Consejo de Administración*. Actualmente compuesto por el Comité de Dirección de *PERSÁN*.
- **Miembros de la Organización:** integrantes del *Consejo de Administración*, miembros de la *Alta dirección*, trabajadores o empleados definidos, temporales o bajo convenio de colaboración, voluntarios de la *Organización* y el resto de las personas bajo subordinación jerárquica de cualquiera de los anteriores.
- **Socios de negocio:** cualquier persona jurídica o física, salvo los *Miembros de la Organización*, con quien la *Organización* mantiene o prevé establecer algún tipo de relación de negocios. A modo enunciativo, pero no limitativo, se incluyen proveedores, clientes y, en general, personas físicas y jurídicas que contratan con *PERSÁN* para la entrega de bienes o prestación de servicios.
- **Tercero:** persona física o jurídica independiente de la *Organización*.
- **Canal Ético / Sistema Interno de Información:** conjunto de medidas adoptadas conforme 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 (o, también referida “Ley de Protección al Informante”) para la gestión de comunicaciones relativas a infracciones de la normativa a la que se refiere dicho texto.

- **Responsable del Sistema Interno de Información:** ha sido designado al *Chief Risk & Compliance Officer*, como encargado de la tramitación diligente de las *Consultas* o *Denuncias* recibidas conforme al *Canal Ético* que debe desarrollar sus funciones con plena autonomía e independencia respecto del resto de los órganos de *PERSÁN*.
- **Comunicación:** declaración por la que cualquier *Miembro de la Organización*, *Socio de negocio* o *Tercero* deja constancia de una cuestión acerca del alcance, interpretación o cumplimiento de la normativa aplicable a la *Organización*. En función de su contenido, una *Comunicación* puede contener una *Consulta* o una *Denuncia*.
- **Consulta:** *Comunicación* por la que cualquier *Miembro de la Organización*, *Socio de negocio* o *Tercero* solicita una aclaración, respuesta o criterio sobre el alcance, interpretación o cumplimiento de la normativa aplicable a *PERSÁN*.
- **Denuncia:** *Comunicación* relativa a un posible *Incumplimiento* de la normativa aplicable a *PERSÁN*.
- **Informante/Denunciante:** persona física o jurídica que interpone una *Consulta* o *Denuncia*. La figura del *Informante* incluye a los *Miembros de la Organización*, *Socios de negocio*, *Terceros* y cualquier persona, con un encaje presente o futuro, en los contextos anteriores.
- **Denunciado:** persona física o jurídica a la que se le imputa un presunto incumplimiento objeto de investigación por parte del *Responsable del Sistema Interno de Información*.
- **Incumplimiento:** comportamiento, activo u omisivo, que supone la infracción de la normativa aplicable a *PERSÁN*. Un *Incumplimiento*, en función de su gravedad, puede abarcar desde el mero *Incumplimiento* formal de un requisito incluido en una norma interna, hasta la comisión de hechos constitutivos de un delito potencialmente imputable a *PERSÁN*.
- **Notificación:** acción de informar a las partes involucradas en el procedimiento, a fin de garantizar el correcto desarrollo del mismo y el respeto a sus derechos.
- **Denuncia de buena fe:** *Denuncia* que se realiza conforme a lo dispuesto en la presente *Política* y está basada en hechos o indicios de los que razonablemente pueda desprenderse la existencia de un *Incumplimiento* de la legislación vigente o de la normativa interna. Se considera que la *Denuncia* es de buena fe cuando la misma se realiza sin ánimo de venganza o de causar un perjuicio laboral o profesional al *Denunciado* o a un *Tercero*.

- **Libro-registro de informaciones:** herramienta utilizada por el *Responsable del Sistema Interno de Información* para asegurar la trazabilidad y seguridad de las *Comunicaciones* recibidas por el *Canal Ético*.
- **Autoridad de Protección al Informante (AAI):** autoridad administrativa independiente, como ente de derecho público de ámbito estatal, que actuará en el cumplimiento de su función principal de protección a los *Informantes*. Entre sus funciones a destacar, se encuentran la gestión de su propio canal externo, la tramitación de procedimientos sancionadores y, la imposición de sanciones, entre otras.
- **Represalia:** acto u omisión prohibido por la ley, o que, de forma directa o indirecta, suponga un trato desfavorable que sitúe al Informante o a las partes involucradas que la sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, solo por su condición en relación con la *Denuncia*, o por haber realizado una revelación pública.
- **Política del Sistema Interno de Información:** conjunto de disposiciones contenidas en el presente documento (en adelante, también referido como la "Política").
- **Procedimiento de Gestión, Investigación y Respuesta de Comunicaciones recibidas a través del Sistema Interno De Información (GIR):** documento que establece los mecanismos necesarios para la *Comunicación* y gestión de manera temprana de cualquier *Incumplimiento*, así como los procedimientos necesarios para la tramitación interna de *Consultas*, y tramitación e instrucción interna de aquellas *Denuncias* o cualquier circunstancia conocida que deba ser investigada.
- **Sistema de Gestión de Compliance penal:** sistema de organización y gestión para la prevención de incumplimientos, cuyo objetivo es la prevención, detección y gestión de riesgos mediante su integración en los procesos de negocio, así como la medición para su mejora continua, y cuya base esencial se representa en la Política de *Compliance* penal y en el Programa de Cumplimiento Normativo. En adelante, también mencionado como el "*Sistema*".
- **Riesgo penal / Riesgo de Compliance:** riesgo relacionado con el desarrollo de conductas que pudieran ser constitutivas de delito/*Incumplimiento* imputable a *PERSÁN* o a cualquiera de las entidades del Perímetro de control.

2. OBJETIVO

El 23 de octubre de 2019 se aprobó la Directiva (UE) 2019/1937, del Parlamento Europeo y del Consejo relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, en adelante, también, "**Directiva Whistleblowing**", cuyo objetivo es reforzar la aplicación del Derecho y las políticas de la Unión en ámbitos específicos mediante el establecimiento de normas mínimas comunes que proporcionen un elevado nivel de protección de las personas que informen sobre infracciones del Derecho de la Unión Europea.

El 20 de febrero de 2023, se aprobó en España la Ley 2/2023 reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, con el objeto de transponer la *Directiva Whistleblowing* (en adelante, "**Ley de protección del informante**"), que entró en vigor el 13 de marzo de 2023.

PERSÁN, en el marco de su *Sistema de Gestión de Compliance penal* y de conformidad con lo establecido en la *Ley de protección del informante*, ha implementado un *Sistema Interno de Información*, por el que cualquier *Miembro de la Organización*, *Socio de negocio* o *Tercero*, que conozca o sospeche de un *Incumplimiento* normativo (bien de la legislación o su normativa de desarrollo, bien de la normativa interna corporativa) cometido por un *Miembro de PERSÁN* o por *Terceros* que estén en contacto con ésta en el marco de sus actividades laborales o profesionales, pueda ponerlo en conocimiento de la *Organización*, de forma identificada o anónima.

El *Sistema Interno de Información* también puede ser empleado para trasladar a *PERSÁN* cualquier *Consulta* relacionada con el alcance, cumplimiento y la interpretación de la normativa aplicable a *PERSÁN*.

PERSÁN reconoce como propios todos los principios recogidos en la *Directiva Whistleblowing* y en la *Ley de protección del informante* y, con el fin de enfatizar dicho compromiso, aprueba la presente *Política del Sistema Interno de Información*, cuyas disposiciones son complementarias a las recogidas en el *Procedimiento de Gestión, Investigación y Respuesta de Comunicaciones recibidas a través del Sistema Interno De Información*.

Esta *Política* tiene como objetivo establecer los principios generales del *Sistema Interno de Información* de *PERSÁN* los derechos que asisten a los *Informantes*, así como el procedimiento que regula el modo en que pueden ponerse en conocimiento del *Responsable del Sistema Interno de Información* los hechos que versen sobre las materias referidas en el apartado siguiente sobre ámbito material de aplicación.

Asimismo, para regular el uso del *Sistema Interno de Información* y el procedimiento de investigación y resolución de las *Comunicaciones recibidas*, *PERSÁN* ha aprobado e implementado el *Procedimiento de Gestión, Investigación y Respuesta de Comunicaciones recibidas a través del Sistema Interno De Información* ("**Procedimiento GIR**"), cuyo contenido se ajusta también a las exigencias de la *Directiva Whistleblowing* y a la *Ley de protección del informante*.

3. ÁMBITO MATERIAL DE APLICACIÓN

La presente *Política* protege a las personas físicas que informen, a través de alguna de las vías establecidas en la siguiente *Política* de:

1. Acciones u omisiones que puedan constituir **infracción del Derecho de la Unión Europea**, siempre que:
 - a. Entren dentro del ámbito de aplicación de los actos de la Unión Europea enumerados en el anexo de 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, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno.
 - b. 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).
 - c. Incidan en el mercado interior, tal y como se contempla en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión Europea 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 con prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades.
2. Acciones u omisiones que puedan ser constitutivas de **infracción penal o administrativa grave o muy grave**.
3. Adicionalmente, el *Sistema Interno de Información* también podrá emplearse para el reporte de las acciones u omisiones que puedan constituir un **Incumplimiento de la normativa interna de la Organización** que no sean constitutivas de infracción del Derecho de la Unión Europea o de infracción penal o administrativa grave o muy grave-, incluidos los principios y valores que asumen como guía de conducta de todos los *Miembros de la Organización*.

Quedan excluidas del ámbito material de aplicación del *Sistema Interno de Información* aquellas *Comunicaciones* relacionadas con cuestiones estrictamente laborales o relacionados con el desempeño profesional (desarrollo de carrera, remuneración, vacaciones, etc.). En esos casos, el asunto se derivará, si así corresponde, al departamento de P&O.

Asimismo, el proceso de *Notificación de Comunicaciones* a través del *Sistema Interno de Información* no deberá utilizarse para informar sobre eventos que supongan una amenaza inmediata para la vida o la propiedad. En estos casos, la situación deberá gestionarse directamente a través de las autoridades competentes o con el teléfono

de emergencias 112. Además, cuando las circunstancias así lo requieran, deberá comunicarse de forma inmediata al superior jerárquico correspondiente.

En esencia, mediante el *Sistema Interno de Información* se podrá comunicar, gozando los *Informantes* de la protección establecida en esta *Política*, cualquier *Incumplimiento* cometido por *Miembros de PERSÁN*, *Socios de negocio* o por *Terceros* no integrantes pero que mantengan relaciones con la *Organización* en el marco de sus labores profesionales, siempre que vayan referidos a los *Incumplimientos* referidos en los numerales 1 y 2 del apartado 3 de la presente *Política* (“**Ámbito material de aplicación**”) – esto es, acciones u omisiones constitutivas de infracciones del Derecho de la Unión Europea o de infracción penal o administrativa grave o muy grave–.

Asimismo, mediante el *Sistema Interno de Información*, cualquier *Miembro de la Organización*, *Socio de negocio* o *Tercero*, podrá reportar acciones u omisiones que puedan constituir un *Incumplimiento* de la normativa interna de la *Organización* – que no sean constitutivas de infracción del Derecho de la Unión Europea o de infracción penal o administrativa grave o muy grave–, incluidos los principios y valores que asumen como guía de conducta de todos los *Miembros de la Organización*, así como trasladar cualquier consulta relacionada con el alcance, cumplimiento y la interpretación de la normativa aplicable a *PERSÁN*.

4. ÁMBITO PERSONAL DE APLICACIÓN

La presente *Política* se extiende, además de a los *Miembros de PERSÁN*, a otros colaboradores tales como voluntarios, becarios, trabajadores en periodos formativos con independencia de que perciban o no una remuneración, candidatos en proceso de selección, trabajadores que hubieran finalizado su relación laboral o mercantil y representantes de los trabajadores, así como a cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores, y a los socios, partícipes y personas pertenecientes al *Consejo de Administración* y a la *Alta Dirección* de *PERSÁN*, que realicen una *Comunicación* a través del *Sistema Interno de Información* de *PERSÁN* sobre cualquiera de las cuestiones señaladas en el apartado 2 de la presente *Política* ("**Ámbito material de aplicación**").

Las medidas de protección previstas en la presente *Política* se aplicarán también, en su caso: (i) a las personas físicas que, en el marco de la organización en la que preste servicios el *Informante*, asistan al mismo en el proceso; (ii) a las personas físicas que estén relacionadas con el *Informante* y que puedan sufrir *Represalias*, como compañeros de trabajo o familiares del *Informante*; y (iii) a las 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.

5. OBLIGACIÓN DE REPORTAR INCUMPLIMIENTOS

Cualquier *Miembro de PERSÁN, Socio de negocio o Tercero* no integrante pero que mantenga relaciones con la *Organización* en el marco de sus labores profesionales (en los términos expuestos en el apartado 3 de la presente *Política*), que tenga conocimiento de algún *Incumplimiento* cometido por cualquier otro *Miembro de la Organización o Socio de negocio*, en un contexto laboral o profesional, podrá inmediatamente comunicarla a través de alguna de las vías establecidas para ello, sin temor a ser sufrir ningún tipo de *Represalia*. En este sentido, se anima a todos los *Miembros de la Organización, Socios de negocio y Terceros* a utilizar los canales habilitados por la *Organización* para la *Comunicación de Incumplimientos*.

El *Sistema Interno de Información*, es el cauce preferente para informar sobre las acciones u omisiones previstas en el apartado 2 de la presente *Política*, siempre que se pueda gestionar de manera efectiva el *Incumplimiento* y el *Informante* considere que no existe riesgo de *Represalias*.

6. COMPOSICIÓN DEL ÓRGANO RESPONSABLE DE LA GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN

El *Consejo de Administración* de la *Organización* ha designado al *Chief Risk & Compliance Officer* como *Responsable del Sistema Interno de Información*, quien tiene concretas facultades de gestión del *Sistema Interno de Información* y de tramitación de expedientes de información, quien ofrece garantías adecuadas de independencia, confidencialidad, protección de datos y secreto de las comunicaciones. La citada designación formal se ha llevado a cabo mediante Acta.

En este sentido, el *Responsable del Sistema Interno de Información* gestionará el *Canal Ético* a través de la *Oficina de Cumplimiento Normativo* de *PERSÁN*, dentro del *Departamento de Risk & Compliance*, la cual está compuesta por:

- *Chief Risk & Compliance Officer.*
- *Compliance Manager.*
- *Equipo de Soporte de Compliance.*

7. VÍAS DE COMUNICACIÓN DEL SISTEMA INTERNO DE INFORMACIÓN

PERSÁN ha habilitado un *Sistema Interno de Información* integrado por las siguientes vías de comunicación:

1. **Comunicaciones escritas**, a través de la plataforma tecnológica habilitada por PERSÁN <https://persan.integrityline.com/>.
2. **Comunicaciones verbales**, solicitando al *Responsable del Sistema Interno de Información* la celebración de una reunión presencial para presentar la *Comunicación*. En tal caso, la citada reunión deberá celebrarse dentro del plazo máximo de siete (7) días naturales desde la solicitud.
3. **A través de un superior jerárquico**, quien tendrá la obligación de trasladar esta *Comunicación* al *Responsable del Sistema Interno de Información* en un plazo que no podrá superar los dos (2) días hábiles desde la recepción de la información, o en su caso, introducir la *Comunicación* recibida, a través de la plataforma indicada en el punto 1 anterior.

En el caso de *Comunicaciones* verbales, previo consentimiento del *Informante*, la conversación entre éste y el *Responsable del Sistema Interno de Información* podrá ser grabada – informándole 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 – (en un soporte seguro, duradero y accesible) o será transcrita de forma exacta por el *Responsable del Sistema Interno de Información*, teniendo derecho el informante a comprobar, rectificar y aceptar la transcripción con su firma.

Independientemente del medio de comunicación utilizado, el *Informante* podrá designar un medio de comunicación preferente para recibir *Notificaciones* sobre el estado de su *Comunicación* o puesta en contacto con el mismo para solicitar información y/o aclaración adicional.

Al margen de lo anterior, cualquier *Comunicación* formal por parte de un órgano judicial o una Administración Pública se considerará medio válido para tomar conocimiento de un *Incumplimiento*.

El *Sistema Interno de Información* **está abierto igualmente a Socios de negocio y a Terceros** ajenos a PERSÁN.

Las *Comunicaciones* se podrán formular tanto de forma **nominativa** como de forma **anónima** (sin introducir datos personales).

Las *Comunicaciones* que se realicen deberán contener, en la medida de lo posible, los siguientes aspectos:

- Contenido mínimo de una *Consulta*:
 - i. Fecha en la que se emite la *Consulta*.

- ii. Nombre y datos de contacto del *Informante* que plantea la *Consulta*, siempre y cuando no se quiera realizar anónimamente. A efectos de facilitar una respuesta sobre la *Consulta*, es recomendable incluir en la *Consulta* la identidad del *Informante*, que se protegerá activamente, de manera que ésta será confidencial.
 - iii. Exposición clara y detallada de la cuestión que requiere aclaración o respuesta, así como del motivo por el que se solicita dicha aclaración, respuesta o criterio.
- Contenido mínimo de una *Denuncia*:
 - i. Fecha de los hechos denunciados.
 - ii. Una exposición clara y lo más detallada posible de los hechos.
 - iii. Identificación del/de la autor/a del hecho, así como de otros/as posibles participantes y las personas que pudieran tener conocimiento sobre el hecho en cuestión.
 - iv. Nombre y datos de contacto del *Informante*, siempre y cuando no se quiera realizar anónimamente.
- En ningún caso, se revelarán datos personales identificativos del *Informante*, más allá del conocimiento de las personas encargadas de la investigación quienes, en cualquier caso, cumplirán con los principios básicos establecidos en la presente *Política*.
- En el caso de contar con asesor externo que preste soporte a la *Oficina de Cumplimiento Normativo* en la gestión del *Sistema Interno de Información*, se exigirá en todo caso que este ofrezca garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones.
- v. Momento en el que se cometió o si se continúa cometiendo el *Incumplimiento* en el momento en el que se está llevando a cabo la *Denuncia*.
 - vi. Cualquier otra información y/o documentación que el *Informante* pueda aportar para la comprensión del hecho en cuestión. La persona encargada de llevar a cabo la investigación podrá requerir la información adicional que deberá ser remitida por el *Informante*.

El *Procedimiento GIR* prevé el proceso de investigación que procederá tras la *Comunicación* de un *Incumplimiento* normativo, alineado con las pautas de la *Directiva Whistleblowing* y de la *Ley de protección del informante*.

En el supuesto de **conflicto de interés**, esto es, que la persona afectada por la *Comunicación* fuera alguno de los *Miembros de la Oficina de Cumplimiento*

Normativo, el *Informante* podrá dirigir la *Comunicación* a la atención de cualesquiera de los otros *Miembros de la Oficina de Cumplimiento Normativo*, quien asumirá entonces la gestión de esta investigación, quedando el *Miembro de la Oficina de Cumplimiento Normativo* afectado recusado de la gestión de dicha *Comunicación*.

Lo mismo sucederá, cuando concurra la incompatibilidad del *Responsable del Sistema Interno de Información* para tratar un asunto concreto, se inhibirá de manera voluntaria, desde su inicio o desde el momento en que se tenga constancia de su involucración en caso de que esta se conociera durante la instrucción. En este sentido, será el *Consejo de Administración* (en caso de *Denuncias* sobre hechos que puedan generar responsabilidad penal para *PERSÁN*) quien decida el/la sustituto/a para el desarrollo del procedimiento.

8. CANALES EXTERNOS DE INFORMACIÓN Y REVELACIÓN PÚBLICA

Sin perjuicio de que el *Sistema Interno de Información* es el cauce preferente para informar sobre las acciones y omisiones constitutivas de infracción contra los derechos de la Unión Europea, o de infracción penal o administrativa grave o muy grave, cualquier persona física podrá acudir directamente:

- Al canal externo de información creado por la *Autoridad Independiente de Protección del Informante, A.I.I.*
 - o En cuanto a asuntos relacionados con el Canal Externo de Información:
canal.externo@proteccioninformante.es (deberá omitir cualquier dato personal de *Terceros* por razones de confidencialidad).
 - o Para asuntos relacionados con el Canal Interno de Información:
canal.interno@proteccioninformante.es (deberá omitir cualquier dato personal de *Terceros* por razones de confidencialidad).
- A la Oficina Europea de Lucha Contra el Fraude: [Denuncia de fraudes - European Anti-Fraud Office - Comisión Europea](#)
- En materia de defensa a la competencia: Denuncia de conducta prohibida / CNMC.
- En materia de infracciones tributarias: Agencia Tributaria: Denuncias.

Tanto las *Comunicaciones* internas, como las *Comunicaciones* realizadas a través de canales externos, gozarán de la protección otorgada en la presente *Política*, siempre que concurren los requisitos expresamente establecidos en el apartado 9 siguiente.

9. PROTECCIÓN A LOS INFORMANTES

En *PERSÁN*, las personas que comuniquen o revelen infracciones de buena fe, **gozarán de todos los derechos de protección** que se prevén en la presente *Política* y en el *Procedimiento GIR*, siempre que:

1. Tengan motivos fundamentados para pensar que la información que comunican a *PERSÁN* es veraz en el momento de la *Comunicación*, y que la citada información entra dentro del ámbito de aplicación material de la *Ley de protección de informantes* – esto es, acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea y acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave –.
2. Hayan realizado la *Comunicación* o revelación conforme a los requerimientos previstos a tal efecto por *PERSÁN* y la *Ley de Protección del Informante*.

Las personas que hayan comunicado o revelado públicamente información sobre acciones u omisiones, de buena fe, a las que se refiere la *Ley de protección del informante* de forma anónima, pero que posteriormente hayan sido identificadas y cumplan las condiciones previstas en este apartado, tendrán derecho a la protección que la *Ley de protección del informante* y la presente *Política* prevén.

Las personas que informen de buena fe ante las instituciones, órganos u organismos pertinentes de la Unión Europea sobre 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 de protección del informante* y en la presente *Política*.

Por el contrario, **no gozarán de la protección** prevista en la presente *Política* y en el *Protocolo GIR*, aquellas personas que comuniquen o revelen:

1. Informaciones contenidas en *Comunicaciones que hayan sido inadmitidas* por alguna de las siguientes razones:
 - a. Cuando los hechos relatados, tras un análisis preliminar, carezcan de toda verosimilitud, debidamente justificado.
 - b. Cuando los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico incluida en el ámbito de aplicación de la *Ley de protección del informante* o ámbito de aplicación de la presente *Política*.
 - c. Cuando la *Comunicación* carezca manifiestamente de fundamento o existan, a juicio del *Responsable del Sistema Interno de Información*, indicios racionales de haberse obtenido mediante la comisión de un delito.
 - d. Cuando la *Comunicación* no contenga información nueva y significativa sobre infracciones objeto de una *Comunicación* anterior respecto de la cual hayan 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 *Responsable del Sistema Interno de Información*, notificará la resolución de manera motivada.

2. 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.
3. Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores.
4. Informaciones que se refieran a acciones u omisiones no comprendidas en el ámbito material de la presente Política.

La inadmisión de la *Comunicación* formulada a través de los canales idóneos habilitados será *Notificada* al *Informante* en un plazo razonable, dentro de los **quince (15) días hábiles** siguientes al acuse de recibo de la *Comunicación*, salvo que la *Comunicación* fuera anónima o el informante hubiera renunciado a recibir *Notificaciones* relativas al procedimiento.

10. PROHIBICIÓN DE REPRESALIAS

PERSÁN adoptará las medidas necesarias para prohibir todo acto constitutivo de *Represalia* o conducta perjudicial, incluidas las amenazas de *Represalia* y las tentativas de *Represalia*, contra las personas que presenten una *Comunicación* referida a acciones u omisiones comprendidas en el ámbito material de aplicación de la presente *Política*.

Se entiende por *Represalia* cualesquiera actos u omisiones que estén prohibidos por la Ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, solo por su condición de *Informantes*, o por haber realizado una revelación pública.

A los efectos de lo previsto en esta *Política*, y a título meramente enunciativo, pero no limitativo, se consideran *Represalias* las siguientes:

1. 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.
2. Terminación anticipada o anulación de contratos de bienes o servicios.
3. Imposición de cualquier medida disciplinaria, degradación o denegación de ascensos.
4. 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.
5. Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.
6. Evaluación o referencias negativas respecto al desempeño laboral o profesional.
7. 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.
8. Denegación o anulación de una licencia o permiso.
9. Denegación de formación.
10. Discriminación, o trato desfavorable o injusto.

Las medidas recogidas en los anteriores numerales 1 a 4, no serán consideradas *Represalia* cuando se lleven 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*.

Asimismo, se hace saber que 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 Independiente de Protección del Informante* que, excepcionalmente y de forma justificada, podrá extender el período de protección, previa audiencia de las personas u órganos que pudieran verse afectados (la denegación de tal extensión del período de protección deberá estar motivada).

Igualmente, se hace saber que los actos 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 de protección del informante*, 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.

Además, los *Informantes* podrán acceder, según corresponda, a las siguientes medidas de apoyo que prestará la *Autoridad Independiente de Protección del Informante* y/o órgano autonómico competente:

1. Información y asesoramiento completos e independientes, que sean fácilmente accesibles para el público y gratuitos, sobre los procedimientos y recursos disponibles, protección frente a *Represalias* y derechos de la persona afectada.
2. Asistencia efectiva por parte de las autoridades competentes ante cualquier autoridad pertinente implicada en su protección frente a *Represalias*, incluida la certificación de que pueden acogerse a protección al amparo de la *Ley de protección del informante*.
3. Asistencia jurídica en los procesos penales y en los procesos civiles transfronterizos de conformidad con la normativa comunitaria.
4. Apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la *Autoridad Independiente de Protección del Informante* y/o órgano autonómico competente, tras la valoración de las circunstancias derivadas de la presentación de la *Comunicación*.

Todo ello, además, con independencia de la asistencia que pudiera corresponder a la persona informante, al amparo de la Ley 1/1996, de 10 de enero, de asistencia jurídica gratuita, para la representación y defensa en procedimientos judiciales derivados de la presentación de la *Comunicación* o revelación pública.

11. MEDIDAS DE PROTECCIÓN FRENTE A REPRESALIAS

PERSÁN adoptará las medidas necesarias para garantizar que los *Informantes* estén protegidos frente a *Represalias*.

A continuación, se exponen y se hace saber a todos los potenciales *Informantes* las principales medidas de protección previstas tanto en la *Directiva Whistleblowing* como en la *Ley de protección del informante*, a los que PERSÁN se adhiere y se compromete a facilitar su efectiva aplicación:

- No se considerará que las personas que comuniquen información sobre las acciones u omisiones recogidas en los numerales 1 y 2 del apartado 3 de la presente *Política* o que hagan una revelación pública de conformidad con la *Ley de protección del informante*, 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 esta *Política* y de la *Ley de protección del informante*, todo ello sin perjuicio de lo dispuesto en el artículo 2.3 de la *Ley de protección del informante*¹. 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.

- 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.
- 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 de protección del informante*, será exigible conforme a la normativa aplicable.
- 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 de protección del informante* 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

¹ Artículo 2.3 de la Ley de protección del informante: “La protección prevista en esta 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”.

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.

- 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, las personas que realicen una *Comunicación* de conformidad con la presente *Política* y la *Ley de protección del informante*, no incurrirán en responsabilidad de ningún tipo como consecuencia de comunicaciones o de revelaciones públicas protegidas por dicha Ley. 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 de protección del informante*.

12. MEDIDAS DE PROTECCIÓN PARA LAS PERSONAS SOBRE LAS QUE VERSA LA COMUNICACIÓN

PERSÁN garantizará que el *Denunciado* o las personas sobre las que versa la *Comunicación* sean oídos en el marco de la investigación interna, tengan derecho a la presunción de inocencia, al derecho de defensa y al derecho de acceso al expediente en los términos regulados en la *Ley de protección del informante*.

Asimismo, la identidad del *Denunciado* o de las personas sobre la que versa la *Comunicación* será protegida y tratada de manera confidencial, al igual que los hechos objeto de *Comunicación*, del mismo modo que la identidad del propio *Informante*, siempre con los límites y excepciones que sea necesario determinar para garantizar el buen fin de la investigación, o la eventual comunicación a las autoridades competentes.

13. SANCIONES

Las sanciones que podrán imponerse a los *Miembros de la Organización* en cada caso serán las previstas en el Estatuto de los Trabajadores, en el Convenio Colectivo que resulte de aplicación o en la legislación laboral aplicable y se graduarán atendiendo a la gravedad de los hechos cometidos, pudiendo tomarse en consideración circunstancias tales como los daños o perjuicios causados, las circunstancias de las víctimas, si las hubiere, entre otros.

Asimismo, también están previstas las posibles sanciones que podrán ponerse a los *Socios de negocio* que lleven a cabo cualquier tipo de *Incumplimiento* en los términos establecidos en la presente *Política*, los cuales, incluyen entre otras, el cese de las relaciones de negocio.

También podrán adoptarse medidas adicionales a las disciplinarias, incluyendo las reclamaciones que correspondan o el reporte de los hechos a las autoridades administrativas, policiales o judiciales que correspondan.

14. CONFIDENCIALIDAD

Sin perjuicio de lo estipulado en otros apartados de la presente *Política*, *PERSÁN* garantiza la confidencialidad de la identidad del *Informante* y de cualquier persona mencionada en la *Comunicación*, y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la protección de datos, impidiendo el acceso de personal no autorizado.

En virtud de lo anterior, el acceso a los datos relativos a la *Comunicación* queda limitado a los miembros específicamente autorizados por *PERSÁN* para recibir, seguir o resolver las *Comunicaciones* recibidas, así como aquellos *Terceros* (por ejemplo, una autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente) cuando constituya una obligación necesaria y proporcionada impuesta por normativa aplicable, en el contexto de una investigación llevada a cabo por las autoridades nacionales o en el marco de un proceso judicial, y, en particular, cuando la revelación pretenda salvaguardar el derecho de defensa de la persona afectada.

En cualquier caso, salvo en los casos previstos, *PERSÁN* garantiza que ninguna persona no autorizada conozca la identidad del *Informante* ni cualquier otra información que pueda ayudar a deducir directa o indirectamente su identidad. En concreto, *PERSÁN* garantiza que el *Denunciado* no será en ningún caso informada de la identidad del *Informante* o, en su caso, de quien haya llevado a cabo la revelación pública.

Asimismo, *PERSÁN* garantiza la confidencialidad de los datos y hechos aportados cuando la *Comunicación* sea remitida por canales que no sean los establecidos o a miembros del personal no responsable de su tratamiento. Para ello, *PERSÁN* ha formado en esta materia adecuadamente a su personal y ha advertido sobre las infracciones por el quebranto del deber de confidencialidad y, asimismo, el establecimiento de la obligación del receptor de la *Comunicación* de remitirla inmediatamente al *Responsable del Sistema Interno de Información*.

En cumplimiento de todo lo anterior, *PERSÁN* ha implantado medidas técnicas y organizativas en el *Sistema Interno de Información*, para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier persona que se mencione en la información suministrada, especialmente la identidad del *Informante*, en caso de que se hubiera identificado.

En relación con las personas afectadas por la *Comunicación*, *PERSÁN* garantiza que durante la tramitación del expediente las personas afectadas por la *Comunicación* tendrán derecho a la misma protección establecida para los *Informantes*, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

Por su lado, quienes reciban revelaciones públicas cuentan con las mismas obligaciones arriba descritas y, en ningún caso obtendrán datos que permitan la identificación del *Informante* y deberán contar con medidas técnicas y organizativas adecuadas.

Las revelaciones hechas en virtud de este apartado estarán sujetas a salvaguardas establecidas en la normativa aplicable y, en particular, se informará al *Informante* antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial. Cuando la autoridad competente lo comunique al *Informante*, le remitirá un escrito explicando los motivos de la revelación de los datos confidenciales en cuestión.

En todo caso, *PERSÁN* velará por que las autoridades competentes que reciban información sobre infracciones que incluya secretos comerciales, no los usen ni revelen para fines que vayan más allá de lo necesario para un correcto seguimiento de las actuaciones.

15. PROTECCIÓN DE DATOS

Los datos personales tratados en aplicación de la presente *Política* y del *Procedimiento GIR*, incluido el intercambio o transmisión de datos personales con las autoridades competentes, serán tratados por *PERSÁN*, con NIF A.91.380.014 y con domicilio en Calle Pino Albar, 2, 41016, Sevilla y e-mail gdpr@persan.es en calidad de responsable del tratamiento de conformidad con lo dispuesto en la normativa sobre protección de datos personales.

Los datos personales facilitados a través del *Sistema Interno de Información* serán tratados para la finalidad de recibir y analizar las acciones u omisiones reportadas y, en su caso, decidir sobre la admisión a trámite y el inicio de una investigación sobre los hechos informados. Adicionalmente, cierta información podrá ser tratada para dejar evidencia del funcionamiento del *Sistema Interno de Información*. En este último supuesto, *PERSÁN* garantiza que la información almacenada como evidencia será anonimizada.

En caso de recibir información que no sea necesaria para la tramitación e investigación de las acciones u omisiones a las que se refiere el apartado 3 de la *Política*, el responsable del tratamiento procederá a su inmediata supresión.

Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la *Ley de protección del informante* y de la presente *Política*, así como aquella información o parte de ella que se acreditara como no veraz, salvo que dicha falta de veracidad pueda constituir un ilícito penal.

El responsable del tratamiento tratará los datos personales facilitados por el *Informante* en cumplimiento de una obligación legal, en concreto, en cumplimiento de la *Ley de protección del informante*. Además, en el caso de *Comunicaciones* realizadas verbalmente, se requerirá el consentimiento del *Informante* para documentar dicha *Comunicación*, incluidas las realizadas a través de reunión presencial, telefónica o mediante mensajería de voz. Por su lado, el tratamiento de datos especialmente protegidos podrá ser tratado por el responsable por razones de un interés público esencial conforme a lo previsto en el artículo 9.2.g) del Reglamento (UE) 2016/679.

En caso de tratamiento de datos personales derivado de una revelación pública, la base jurídica que lo legitima es que el mismo 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 11 de 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).

Los datos personales recabados a través del *Sistema Interno de Información* se conservarán de conformidad con lo dispuesto en la legislación aplicable. En concreto, por lo dispuesto en el artículo 32.4 de la citada Ley 2/2023 y por el artículo 24.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y

garantía de los derechos digitales, transcurridos tres (3) meses desde la recepción de la *Comunicación* sin que se hubiesen iniciado actuaciones de investigación, se procederá a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema, en cuyo caso se mantendrán anonimizados.

No obstante, en caso de que fuese necesario tratar los datos personales durante más tiempo para continuar la investigación o, en su caso, porque se considere necesario iniciar las acciones legales oportunas, los datos se conservarán, en tanto sea necesario para concluir la investigación o para el ejercicio de las correspondientes acciones por parte de *PERSÁN*.

Para cumplir con las finalidades arriba descritas, el responsable del tratamiento puede facilitar el acceso a los datos personales a:

- Terceras empresas que presenten servicios, tales como asesores y colaboradores externos que presten soporte en la gestión o, en su caso, investigación de las *Comunicaciones* recibidas a través del *Sistema Interno de Información*.
- Aquellas áreas o departamentos relevantes de cara a la tramitación de la *Comunicación* y, en su caso, para la investigación y las posibles medidas a tomar con respecto a la conducta comunicada siempre y cuando resulte necesario.
- Igualmente, los datos personales podrán ser cedidos a los Jueces y Tribunales, al Ministerio Fiscal, así como a las Administraciones Públicas competentes como consecuencia de la investigación que se pueda poner en marcha.

En relación con lo anterior, *PERSÁN* informa a los interesados de que no realiza transferencias internacionales de los datos personales facilitados.

No obstante, *PERSÁN* informa de que, en caso de que el *Denunciado* al que se refieran los hechos relatados en la *Comunicación* o a la que se refiera la revelación pública, ejerciese el derecho de oposición, se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales.

Sin perjuicio de los derechos que le correspondan al informante, de acuerdo con la normativa sobre protección de datos, en caso de haber realizado la *Comunicación* de manera verbal, *PERSÁN* ofrece la oportunidad de solicitar el acceso a sus datos personales, rectificación, supresión o cancelación, la limitación del tratamiento, oposición o la portabilidad de los mismos enviando una solicitud por escrito dirigida a *PERSÁN*, S.A., en calle Pino Albar, nº 2 – C.P. 41016 Sevilla, o bien enviando un correo electrónico a gdpr@persan.es. Podremos solicitarle una copia de su DNI en caso de que sea necesario para acreditar su identidad.

Por otro lado, se informa al interesado de que, bajo las condiciones que se establecen en la normativa aplicable, podrá ejercitar los derechos reconocidos en la normativa

de protección de datos mediante el envío de una *Comunicación* a través del *Sistema Interno de Información*.

Asimismo, los interesados tienen el derecho a presentar una reclamación ante la Agencia Española de Protección de Datos , bien a través de su sede electrónica (en www.aepd.es) o en su domicilio, en calle Jorge Juan, nº 6, C.P. 28001 de Madrid.

El *Responsable del Sistema Interno de Información* revisará periódicamente el correcto funcionamiento del *Sistema Interno de Información* y de las disposiciones de la presente *Política*.

16. PRINCIPIOS BÁSICOS DEL PROCEDIMIENTO GIR

El *Procedimiento GIR* se rige por los siguientes principios, que serán observados durante la tramitación de cualquier expediente:

- **Confidencialidad:** el *Procedimiento GIR* garantizará el carácter confidencial de la identidad del *Informante*, de cualquier persona mencionada en la *Comunicación* y de los datos relativos al incidente comunicado, salvo *Comunicación* a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.
- **Imparcialidad:** el *Responsable del Sistema Interno de Información* ha de regirse en todo caso por el principio de imparcialidad, otorgando un trato homogéneo a todas las *Comunicaciones*, con independencia de las personas implicadas y evitando cualquier tipo de conflicto de interés.
- **Objetividad:** se investigará, no sólo los hechos y circunstancias que establecen y agravan la responsabilidad del *Denunciado*, sino también los que le eximan de ella o la extingan o atenúen.
- **Independencia del Responsable del Sistema Interno de Información:** el *Responsable del Sistema Interno de Información* gozará de plena independencia y autonomía para acordar la práctica de las diligencias que estime necesarias para el esclarecimiento de los hechos comunicados, persiguiendo en todo caso la búsqueda de la verdad.
- **Documentación:** cada *Comunicación* dará lugar a un expediente, en el que el *Responsable del Sistema Interno de Información* incluirá la documentación detallada de todo el procedimiento de investigación.
- **Buena fe:** lo dispuesto en el *Procedimiento GIR* y en esta *Política* deberá ser interpretado conforme a los principios y exigencias de la buena fe.
- **Proporcionalidad:** este principio responde a la necesidad de que la sanción se ajuste a la gravedad de los hechos, evitando que ésta sea una medida desproporcionada.
- **Principio del “debido proceso”:** toda persona tiene derecho a ser oído y a hacer valer sus pretensiones legítimas frente a los encargados de la investigación.

17. REGISTRO DE COMUNICACIONES

PERSÁN llevará un registro de todas las comunicaciones y consultas que pueda recibir a través del *Sistema Interno de Información*, recopiladas en el llamado "**libro-registro**", cumpliendo en todo momento con los requisitos de confidencialidad establecidos, y durante el tiempo estrictamente necesario y proporcionado para dar cumplimiento a los requisitos legales y normativos procedentes de la Unión Europea.

Cuando la *Comunicación* se haya realizado de forma verbal, *PERSÁN* se reserva el derecho a documentar la *Comunicación* verbal de una de las siguientes maneras:

- Mediante una grabación de la conversación en un formato duradero y accesible, previo consentimiento del *Informante*.
- A través de una transcripción completa y exacta de la conversación realizada por el *Responsable del Sistema Interno de Información*.

En todo caso, el *Informante* tiene derecho a comprobar, rectificar y aceptar mediante su firma, la transcripción realizada. En caso de que el *Informante* se negase a firmar la transcripción, el *Responsable del Sistema Interno de Información* podrá acudir con un testigo.

Cuando el *Informante* haya solicitado una entrevista personal con el *Responsable del Sistema Interno de Información* para realizar la *Comunicación*, *PERSÁN* garantizará, a reserva del consentimiento del *Informante*, que se conserven registros completos y exactos de la reunión mantenida, en un formato duradero y accesible.