PROCEDIMIENTO CORPORATIVO DE GESTIÓN, INVESTIGACIÓN Y RESPUESTA DE COMUNICACIONES RECIBIDAS A TRAVÉS DEL SISTEMA INTERNO DE INFORMACIÓN

persán

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.	08/08/2024	Aprobación por parte del Consejo de Administración: actualización Fase 1 proceso certificador del Sistema de Gestión *Compliance* penal según UNE 19601:2017.
3.0.	25/09/2025	Aprobación por parte del Consejo de Administración: actualización del *Sistema de Gestión de Compliance penal* (cambios organizativos).
4.0	02/09/2026	Aprobación por parte del *Consejo de Administración*: Despliegue internacional del Sistema Interno de Información.

ÍNDICE

1. DEFINICIONES ..... ¡ERROR! MARCADOR NO DEFINIDO.
2. OBJETIVO 9
3. ÁMBITO DE APLICACIÓN 10
4. VÍAS DE COMUNICACIÓN Y CONTENIDO DE LAS COMUNICACIONES 11
4.1 Medios para realizar la *Comunicación* 11
4.2 Contenido mínimo de las *Comunicaciones* 11
4.3 Canales Externos de Información y Comunicación a las autoridades competentes 12
5. IDONEIDAD, INDEPENDENCIA Y CONFLICTOS DE INTERÉS 14
6. CONFIDENCIALIDAD 15
7. MEDIDAS DE PROTECCIÓN PARA LAS PERSONAS AFECTADAS POR LA COMUNICACIÓN 17
8. PROHIBICIÓN DE REPRESALIAS Y PROTECCIÓN AL INFORMANTE 18
9. RECEPCIÓN DE LAS COMUNICACIONES Y FORMACIÓN DEL EXPEDIENTE 20
9.1 Acuse de recibo 20
9.2 Solicitud de ampliación de la información recibida 20
9.3 Formación de expediente inicial 20
9.4 Tratamiento de las Comunicaciones relacionadas sobre acoso 20
9.4.1 Recepción y remisión de las Comunicaciones sobre acoso 21
9.4.2 Garantías sobre las Comunicaciones sobre acoso 21
9.4.3 Trazabilidad y protección de datos en las Comunicaciones sobre acoso 22
10. ANÁLISIS Y DECISIÓN PRELIMINAR SOBRE LA COMUNICACIÓN RECIBIDA 23
10.1 Análisis preliminar de la comunicación recibida 23
10.2 Decisión preliminar sobre la información recibida 23
10.3 Medidas cautelares 24
11. PROCEDIMIENTO DE INVESTIGACIÓN INTERNA 25
11.1 Elección de la estrategia de investigación 25
11.2 Planificación de la investigación 25
11.3 Comunicación a los sujetos afectados 27
11.4 Desarrollo de la investigación 27
11.5 Documentación del procedimiento de investigación 28
11.6 Informe final 28
11.7 Actuaciones finales 29
12. CONCLUSIÓN DEL PROCEDIMIENTO 30
12.1 Órgano responsable 30
12.2 Trámite de audiencia 30

12.3 Decisiones del Responsable del Sistema Interno de Información 30
12.4 Sanciones 30
12.5 Otras medidas 31
12.6 Comunicación de las decisiones 31
13. CONSERVACIÓN DE LA DOCUMENTACIÓN 32
13.1 Plazos de conservación 32
13.2 Registro de comunicaciones 32
14. PROTECCIÓN DE DATOS PERSONALES 34
14.1 Principios Generales 34
14.2 Responsables del tratamiento 34
14.3 Categorías de datos tratados 34
14.4 Finalidades del tratamiento y bases legitimadoras 34
14.5 Confidencialidad 35
14.6 Conservación de los datos 35
14.7 Destinatarios de los datos 36
14.8 Transferencias internacionales de datos 36
14.9 Derechos de los interesados 37
15. DIFUSIÓN, REVISIÓN Y ACTUALIZACIÓN DEL PROCEDIMIENTO 38

1. DEFINICIONES

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

- ***Grupo Persán / la Organización***: se entiende por tal al conjunto de todas aquellas sociedades en las que *PERSÁN*, S.A. posee una participación, directa o indirectamente, de más del 50% de su capital social.

- ***PERSÁN / la Compañía***: incluye a la sociedad matriz del *Grupo Persán*, Persán, S.A.

- ***Oficina de Cumplimiento Normativo / Oficina de Compliance***: órgano interno colegiado del *Grupo Persán*, dotado de la suficiente autoridad y de poderes autónomos de iniciativa y control, responsable de supervisar el adecuado funcionamiento y observancia del *Sistema de Gestión de Compliance penal* de la *Organización*, tanto en territorio nacional como internacional.

  La *Oficina de Compliance* vela por la correcta identificación, prevención y gestión de los *Riesgos de Compliance*, con especial atención a los *Riesgos penales*, asegurando la adecuación del *Sistema* a lo dispuesto en la normativa local aplicable en los países en los que el *Grupo Persán* desarrolla su actividad y a las mejores prácticas internacionales, entre ellas la Norma ISO 37301:2021.

- ***Consejo de Administración***: órgano que tiene la responsabilidad y autoridad fundamental de las actividades, la gobernabilidad y las políticas de *Grupo Persán* y al que la *Alta dirección* informa y rinde cuentas.

- ***Alta dirección / Comité de Dirección***: es el órgano de alto nivel dentro de *Grupo Persán* que depende directamente del *Consejo de Administración*. Actualmente compuesto por el *Comité de Dirección* de *Grupo Persán*.

- ***Miembros de la Organización***: integrantes del *Consejo de Administración*, miembros de la *Alta dirección*, trabajadores o empleados indefinidos, 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 *Grupo 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 en la *Organización* conforme a la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión; la Normativa de Protección al Informante aplicable en cada país que transpone dicha Directiva, incluida, en el caso de España, 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; y, los principios de la Norma ISO 37002:2021, sobre Sistemas de Gestión de la Denuncia de Irregularidades, para la gestión de *Comunicaciones* relativas a infracciones de la normativa a la que se refiere dicho texto.

- ***Responsable del Sistema Interno de Información***: se ha designado al *Chief Risk & Compliance Officer*, como encargado de la tramitación diligente de *Comunicaciones* recibidas conforme al *Canal Ético* que debe desarrollar sus funciones con plena autonomía e independencia respecto del resto de los órganos de *Grupo Persán*. El *Responsable del Sistema Interno de Información* tiene la potestad delegada del propio *Consejo de Administración* de *Grupo Persán* de nombrar *Delegados Locales* que le asistan en la gestión de las *Comunicaciones* recibidas por el *Sistema Interno de Información*.

- ***Delegado Local:*** órgano interno de carácter unipersonal o colegiado, formalmente designado por la *Oficina de Compliance*, al cual se le confía, con carácter general, la responsabilidad de observar el funcionamiento y observancia del *Sistema de Gestión de Compliance penal* de *Grupo Persán*, únicamente dentro de su ámbito de actuación geográfico. Cuando el *Chief Risk & Compliance Officer*, en su condición de *Responsable del Sistema Interno de Información (RSII)*, designe adicionalmente a esta misma persona para apoyar la gestión operativa del Sistema Interno de Información en dicha jurisdicción, dicha designación específica y sus funciones se regirán por lo dispuesto en la *Política Corporativa del Sistema Interno de Información* y el *Procedimiento GIR*, sin que ambas designaciones deban confundirse ni implicar necesariamente el mismo alcance de facultades ni el mismo órgano designante.

  En este sentido, quedan diferenciadas las figuras del *Delegado Local del SGCP*, para funciones estrictamente relacionadas con el *SGCP* y del *Delegado Local del SII*, para funciones estrictamente relacionadas con el *SII*.

  Los *Delegados Locales* deberán contar con autorización expresa y por escrito del órgano que en cada caso lo designe, suscribir el correspondiente compromiso de confidencialidad, reunir condiciones adecuadas de idoneidad profesional e independencia funcional respecto de las áreas operativas y de negocio de la *Organización*, así como cualquier otro documento requerido por la normativa local aplicable. La designación no implicará la transferencia de la responsabilidad del *Sistema*, que corresponderá en todo caso a la *Oficina de Compliance*.

- ***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 externa aplicable a la *Organización*, así como de la normativa corporativa interna de 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 *Grupo Persán* y/o corporativa.

- ***Denuncia:*** *Comunicación* relativa a un posible *Incumplimiento* de la normativa externa aplicable a la *Organización*, así como de la normativa corporativa interna de la *Organización*.

- ***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 afectada por la Denuncia***: 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***: conductas irregulares o potenciales actos ilícitos o contrarios a la ley o a la normativa interna corporativa (incluyendo, en particular, cualquier conducta que pudiera constituir un delito, una infracción administrativa grave o muy grave, o una infracción del derecho de la Unión Europea).

- ***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.

- ***Riesgo penal:*** riesgo relacionado con el desarrollo de conductas que pudieran ser constitutivas de delito, según el régimen de responsabilidad penal o cuasi penal de las personas jurídicas establecido en la legislación local que corresponda a cada jurisdicción donde opera el *Grupo Persán*.

- ***Denuncia de buena fe***: *Denuncia* que se realiza conforme a lo dispuesto en la *Política Corporativa del Sistema Interno de Información* 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*.

- ***Represalia / Conducta perjudicial***: 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 Corporativa del Sistema Interno de Información***: documento corporativo que establece los principios que rigen el *Sistema Interno de Información* de la *Organización*, así como establece los derechos y obligaciones de los usuarios del mismo (en adelante, también referido como la "***Política***").

- ***Procedimiento Corporativo de Gestión, Investigación y Respuesta de Comunicaciones recibidas a través del Sistema Interno de Información (GIR)***: documento corporativo, integrado por el propio documento y sus Anexos de adaptación local, que establecen 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.

Los Anexos locales forman parte integrante del *Procedimiento GIR* y desarrollan las particularidades y requisitos específicos exigidos por la normativa aplicable en cada jurisdicción donde opere *Grupo Persán* (en adelante, el documento y sus anexos en su conjunto serán también referido como el "***Procedimiento GIR***").

- ***Sistema de Gestión de Compliance penal/SGCP***: 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*.

- ***Normativa de Protección al Informante***: conjunto de disposiciones legales aplicables en cada jurisdicción destinadas a regular la comunicación de infracciones, la protección de los Informantes y la gestión de los sistemas internos de información.

- ***Conflicto de Interés***: Situación en la que existe un interés personal (de carácter financiero, relacional, profesional o de cualquier otra índole) u organizacional, directo o indirecto, que puede comprometer o aparentar comprometer la capacidad de actuar de forma imparcial de una persona en el cumplimiento de sus deberes profesionales y en la defensa del mejor interés de la *Organización.*

2. OBJETIVO

Grupo Persán, en el marco de su *Sistema de Gestión de Compliance penal* y de conformidad con lo establecido en las *best practices* internacionales, tales como la Norma ISO 37002:2021, y en concreto, en la *Directiva Whistleblowing* y la *Normativa de Protección al Informante*, ha implementado un *Sistema Interno de Información*, por el que cualquier M*iembro 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 Grupo 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 *Grupo Persán* cualquier *Consulta* relacionada con el alcance, cumplimiento y la interpretación de la normativa externa aplicable a la *Organización*, así como de la normativa corporativa interna de la *Organización*.

Para ello, *Grupo Persán* ha aprobado una *Política Corporativa del Sistema Interno de Información* que recoge los principios generales que rigen el *Sistema Interno de Información* y la protección de los *Informantes*.

De forma complementaria, el presente *Procedimiento GIR* desarrolla el marco operativo aplicable a la gestión de las *Comunicaciones* recibidas a través del *Sistema Interno de Información*, definiendo las actuaciones, responsabilidades, plazos, garantías y mecanismos de seguimiento que deberán observarse durante la recepción, análisis, investigación y resolución de *Consultas* y *Denuncias*.

Asimismo, el *Procedimiento GIR* incorpora los Anexos locales correspondientes a los requisitos normativos relativos al Sistema Interno de Información de cada jurisdicción en la que opera *Grupo Persán*, los cuales forman parte integrante del mismo y tienen por finalidad adaptar las disposiciones corporativas aquí contenidas a las particularidades, requisitos y obligaciones establecidos por la *Normativa de Protección al Informante*.

En consecuencia, el presente *Procedimiento GIR* establece los criterios corporativos comunes que deberán aplicarse en todo el *Grupo Persán*, garantizando una gestión homogénea, coordinada, trazable y conforme a Derecho de las *Comunicaciones*, sin perjuicio de las especialidades locales recogidas en los Anexos locales correspondientes.

Todo ello con el objetivo de asegurar la adecuada detección, comunicación, investigación y respuesta frente a posibles *Incumplimientos*, garantizando la confidencialidad, la independencia, la protección del *Informante*, los derechos de las personas afectadas y el cumplimiento de la normativa aplicable en cada jurisdicción.

3. ÁMBITO DE APLICACIÓN

Este *Procedimiento* será de aplicación a todas las *Comunicaciones* recibidas en el *Sistema Interno de Información,* por cualquiera de las vías de comunicación habilitadas en el marco del *Canal Ético*.

Asimismo, el presente *Procedimiento* afecta a todos los *Miembros de la Organización* de modo que deberán cumplir con su contenido, independientemente de la posición de la función que desempeñen, así como la jurisdicción donde se encuentren; así como a cualquier persona que pretenda comunicar un posible *Incumplimiento* que se haya podido producir en un contexto profesional.

En este sentido, el *Procedimiento* vincula a los *Socios de negocio* y *Terceros* que tengan conocimiento de que se ha producido un *Incumplimiento* en su relación con *Grupo Persán*.

Las *Comunicaciones* recibidas podrán versar sobre cualquier *Incumplimiento* de la ley o de la normativa interna de *Grupo Persán*. No obstante, en línea con lo establecido en la *Política*, quedan excluidas del ámbito de aplicación del presente *Procedimiento* aquellas *Comunicaciones* relacionadas con cuestiones estrictamente laborales, aquellas relacionados con el desempeño profesional o aquellas cuyo ámbito de aplicación corresponda específicamente a otra área u órgano de la *Organización*.

El presente *Procedimiento* se aplicará sin perjuicio de lo dispuesto en las especificidades locales contenidas en los Anexos locales que resulten procedentes en aplicación de la ley aplicable en las jurisdicciones en los que el *Grupo Persán* opera. En caso de contradicción entre lo dispuesto en los Anexos locales y lo dispuesto en la normativa local, respecto de lo dispuesto en el presente *Procedimiento GIR*, prevalecerá lo dispuesto en el procedimiento de dicho Anexo local o especificación local.

La aplicación del presente *Procedimiento GIR* en ningún caso podrá suponer el incumplimiento de las disposiciones legales vigentes o de las particularidades previstas en los Anexos locales de los países donde el Grupo Persán opera. Tales disposiciones locales se aplicarán, en todo caso, con prevalencia al *Procedimiento GIR*. En ausencia de disposiciones legales vigentes en el mercado que corresponda, o como complemento de las que existan, resultará de aplicación el contenido del presente *Procedimiento*, que se aplicará sin perjuicio de lo dispuesto en la *Política* y del resto de normativa interna del *Grupo Persán* que resulte de aplicación.

4. VÍAS DE COMUNICACIÓN Y CONTENIDO DE LAS COMUNICACIONES

4.1 Medios para realizar la *Comunicación*

Grupo 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 *Grupo Persán* https://persán.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 igualmente abierto a *Socios de negocio* y a *Terceros*** ajenos a *Grupo Persán*.

Las *Comunicaciones* se podrán formular tanto de forma **nominativa** como **anónima**.

4.2 Contenido mínimo de las *Comunicaciones*

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 *Política Corporativa del Sistema Interno de Información*.

En el caso de contar con asesor externo que preste soporte a la *Oficina de Compliance* 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* y sus Anexos locales prevén el proceso de investigación que deberá seguirse tras la recepción de una *Comunicación* de un *Incumplimiento* normativo, alineado con las *Best Practices* internacionales, la *Directiva Whistleblowing* y la *Normativa de Protección al Informante*.

4.3 Canales Externos de Información y Comunicación a las autoridades competentes

Sin perjuicio de que el *Sistema Interno de Información* es el cauce preferente para informar sobre las acciones y omisiones constitutivas de infracciones del Derecho de la Unión Europea, o de una infracción penal, cuasi penal o administrativa grave o muy grave, cualquier persona podrá asimismo hacer uso de los canales externos habilitados por las autoridades competentes, de conformidad con la normativa aplicable en cada caso, incluyendo, cuando corresponda, ante las instituciones, órganos u organismos de la Unión Europea, para informar sobre acciones u

omisiones susceptibles de ser incluidas en el ámbito material de la *Directiva Whistleblowing* y, en su caso, de las respectivas normas locales que resulten aplicables.

En concreto, en el caso de la jurisdicción española, podrán acudir a los siguientes canales:

- Canal externo de información creado por la *Autoridad Independiente de Protección del Informante, A.I.I.*
    - 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).
    - Para asuntos relacionados con el canal interno de información:

      canal.interno@proteccioninformante.es (deberá omitir cualquier dato personal de *Terceros* por razones de confidencialidad).
- 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 el presente *Procedimiento* y sus Anexos locales.

5. IDONEIDAD, INDEPENDENCIA Y CONFLICTO DE INTERÉS

El *Responsable del Sistema Interno de Información*, los miembros de la *Oficina de Compliance* y los *Delegados Locales* deberán reunir, en el ejercicio de sus funciones en relación con el *Sistema*, idoneidad profesional e independencia funcional respecto de las áreas operativas y de negocio susceptibles de ser objeto de una *Comunicación*. Adicionalmente, el *Responsable del Sistema Interno de Información* desarrollará sus funciones con plena autonomía respecto del resto de los órganos de la *Organización*, sin recibir instrucciones de ningún tipo en su ejercicio, y la *Organización* garantizará que disponga de los medios personales y materiales necesarios para ello.

El *Responsable del Sistema Interno de Información* verificará el cumplimiento de estas condiciones por los miembros de la *Oficina de Compliance* y por los *Delegados Locales* en el momento de su designación y con periodicidad anual; el *Consejo de Administración* realizará la misma verificación respecto del propio *Responsable del Sistema Interno de Información*.

En el supuesto de ***Conflicto de interés***, esto es, que la persona afectada por la *Comunicación* fuera el *Responsable del Sistema Interno de Información*, alguno de los *Miembros de la Oficina de Compliance* o, en su caso, un *Delegado Local* que esté interviniendo en la gestión de dicha *Comunicación*, la persona afectada deberá abstenerse de participar en la tramitación e investigación del expediente. En tal caso, el *Responsable del Sistema Interno de Información* designará a otro *Miembro de la Oficina de Compliance* o *Delegado Local* no afectado para asumir 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* quien decida el/la sustituto/a para el desarrollo del procedimiento.

Asimismo, con carácter general, cualquier persona que intervenga en la recepción, análisis, investigación o resolución de una *Comunicación* —incluidos el *Responsable del SII*, los miembros de la *Oficina de Compliance* y los *Delegados Locales*— deberá abstenerse cuando concurra respecto de cualquiera de los sujetos implicados: (i) subordinación jerárquica directa o dependencia funcional u organizativa relevante, aunque no exista subordinación jerárquica directa; (ii) parentesco por consanguinidad o afinidad hasta el segundo grado; (iii) amistad íntima o enemistad manifiesta; o (iv) interés personal, directo o indirecto, en el resultado de la investigación. La persona afectada comunicará la causa de abstención al órgano inmediatamente superior en la estructura del *Sistema* (el *Responsable del SII*, o el *Consejo de Administración* si la causa afecta al propio *Responsable del SII*), quien reasignará la gestión.

Cuando la persona afectada por la *Denuncia* sea algún miembro del *Consejo de Administración*, será la *Oficina de Compliance* quien lleve a cabo la pertinente investigación, debiendo reportar de la misma a otro consejero no afectado.

6. CONFIDENCIALIDAD

Sin perjuicio de lo estipulado en otros apartados del presente *Procedimiento* y de los Anexos locales, *Grupo 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 *el Responsable del Sistema Interno de Información* 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 la 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, *Grupo 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, *Grupo Persán* garantiza que el *Denunciado* no será en ningún caso informado de la identidad del *Informante* o, en su caso, de quien haya llevado a cabo la revelación pública.

Asimismo, *Grupo 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, *Grupo 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, *Grupo 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*, *Grupo 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 local 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, *Grupo 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.

7. MEDIDAS DE PROTECCIÓN PARA LAS PERSONAS AFECTADAS POR LA COMUNICACIÓN

Grupo Persán garantizará que las personas *Denunciadas* sean oídas en el marco de la investigación interna empresarial, gocen del derecho a la presunción de inocencia, del derecho de defensa y del derecho de acceso al expediente en los términos permitidos en la *Normativa de Protección al Informante,* así como el resto de principios y derechos que les amparan establecidos en el *Procedimiento GIR*.

Asimismo, la identidad de la persona sobre la que verse la *Comunicación* será protegida y tratada de manera confidencial, al igual que los hechos objeto de *Comunicación* y la identidad del propio *Informante*, en los términos previstos en el apartado "*Confidencialidad*" del presente *Procedimiento*.

8. PROHIBICIÓN DE REPRESALIAS Y PROTECCIÓN AL INFORMANTE

Grupo 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 *Normativa de protección al informante*, a los que *Grupo 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 el apartado "*ámbito material de aplicación*" de la *Política Corporativa del Sistema Interno de Información* o que hagan una revelación pública de conformidad con la *Normativa de protección al 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 este *Procedimiento,* sus Anexos locales y de la *Normativa de protección al informante*. Esta medida no afectará a las responsabilidades de carácter penal o cuasi 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 local vigente.

- 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 *Normativa de Protección al Informante*, será exigible conforme a la normativa local 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 *Normativa de Protección al 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 a la persona que haya tomado la *Conducta 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 el presente *Procedimiento,* sus Anexos locales y la *Normativa de protección al 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 *Normativa de Protección al Informante*.

9. RECEPCIÓN DE LAS COMUNICACIONES Y FORMACIÓN DEL EXPEDIENTE

9.1 Acuse de recibo

Tras la recepción de cualquier *Comunicación* a través del *Sistema Interno de Información*, el *Responsable del Sistema Interno de Información* acusará recibo de la *Comunicación* en el plazo máximo de siete (7) días naturales desde su recepción, salvo que dicha acción pudiera poner en peligro la confidencialidad de la *Comunicación*.

En el acuse de recibo se incluirá una primera capa de información sobre el tratamiento de los datos personales de acuerdo con lo recogido en el apartado "*Protección de datos*" del presente Procedimiento.

Asimismo, se informará al *Informante*, de forma expresa, de que su identidad (en el caso de que se haya identificado) será en todo caso preservada y que no se comunicará a las personas a las que se refieren los hechos relatados ni a *Terceros*.

Del mismo modo, en línea con lo dispuesto en la *Política Corporativa del Sistema Interno de Información*, se hará mención expresa de qué órgano se encargará de gestionar la *Comunicación*, pudiendo ser tanto el *Delegado Local*, como la *Oficina de Compliance* en los supuestos previstos en el apartado "*Distribución de Competencias*" de la citada *Política*.

Dicha distribución de competencias se refiere exclusivamente a la gestión del *Sistema Interno de Información* y no prejuzga el órgano competente para la instrucción y resolución del fondo del asunto cuando, conforme a este *Procedimiento* (por ejemplo, en el apartado "*Tratamiento de las Comunicaciones relacionadas sobre acoso*" o a la normativa interna aplicable, dicha competencia corresponda a otro departamento u órgano de la *Organización.*

9.2 Solicitud de ampliación de la información recibida

En caso de que la información recibida se considere insuficiente, el *Responsable del Sistema Interno de Información* solicitará, al tiempo de acusar recibo – o incluso con posterioridad –, la ampliación de la misma al *Informante*. Es aconsejable que en la solicitud que se remita se detallen los aspectos concretos de la información facilitada que deben ser ampliados. En este trámite no será necesaria información exhaustiva sobre el *Incumplimiento* comunicado, sino sólo la estrictamente imprescindible para la formación y gestión preliminar del expediente.

9.3 Formación de expediente inicial

Con la información recibida, el *Responsable del Sistema Interno de Información* formará un expediente individual para cada caso, que será convenientemente numerado y clasificado con un código de identificación y la fecha de registro, a efectos de su mejor identificación dentro del *Libro-registro* regulado en el apartado "*Registro de comunicaciones*".

En caso de recibirse diferentes comunicaciones sobre un mismo hecho o sobre hechos vinculados, el *Responsable del Sistema Interno de Información* podrá acumular los distintos expedientes.

9.4 Tratamiento de las Comunicaciones relacionadas sobre acoso

Las *Comunicaciones* relativas a acoso laboral, acoso sexual, acoso por razón de sexo o situaciones de discriminación podrán recibirse a través del *Sistema Interno de Información*, que actúa como vía de comunicación según lo establecido en la normativa interna de la *Organización*.

La utilización del *Sistema Interno de Información* como canal de entrada no atribuye al *Responsable del Sistema Interno de Información* competencias para la instrucción, investigación o resolución de estos asuntos, que corresponderán exclusivamente al Departamento de *People & Organization* (*P&O*), de conformidad con lo dispuesto en la normativa interna.

En aquellas jurisdicciones locales que dispongan de su propia normativa en materia de acoso, se estará a lo dispuesto en dicha normativa y en los protocolos locales que resulten de aplicación. En ausencia de normativa o protocolo local específico, se aplicará supletoriamente el presente *Procedimiento GIR* y la remisión se realizará al Departamento de *P&O* de *la Compañía*, que podrá apoyarse en los *Delegados Locales* para la gestión operativa.

Estas *Comunicaciones* deberán ser derivadas al Departamento de *P&O* en el plazo de siete (7) días naturales desde la finalización del análisis preliminar mencionado en el siguiente apartado "*Análisis preliminar de la comunicación recibida*", salvo que de este análisis preliminar pueda interpretarse la existencia de un ilícito penal o de algún *Conflicto de interés*.

9.4.1 Recepción y remisión de las Comunicaciones sobre acoso

Recibida la *Comunicación*, se verificará durante el análisis preliminar si los hechos comunicados versan, total o parcialmente, sobre una situación de acoso laboral, acoso sexual, acoso por razón de sexo o discriminación.

En caso de concluir que la *Comunicación* debe tramitarse conforme a la normativa interna especifica en esta materia, se acordará su remisión al Departamento de *People & Organization* como decisión preliminar, de conformidad con lo previsto en el apartado "***Decisión preliminar sobre la información recibida***" de este *Procedimiento*, trasladando únicamente la información mínima necesaria para su tramitación.

La remisión tendrá carácter meramente administrativo y no implicará valoración sobre el fondo de los hechos ni el ejercicio de facultades de investigación por parte del *Responsable del Sistema Interno de Información.* Al respecto, se procederá a documentar mediante acta motivada y se comunicará al *Informante* —salvo *Comunicación* anónima o renuncia a recibir *Notificaciones*—, indicándole el órgano que asumirá la instrucción.

9.4.2 Garantías sobre las Comunicaciones sobre acoso

La recepción de la *Comunicación* a través del *Sistema Interno de Información* no afectará a las garantías reconocidas al *Informante*: la confidencialidad de su identidad y la protección frente a *Represalias* previstas en la *Política Corporativa del Sistema Interno de Información* y en este *Procedimiento* continúan amparándole durante y con posterioridad a la tramitación por *P&O*.

El *Responsable del Sistema Interno de Información* conserva el papel de garante de dichas protecciones y podrá recabar información sobre el estado del asunto a estos solos efectos.

Cuando la *Comunicación* de acoso concurra con hechos que excedan el ámbito del citado Protocolo contra el acoso — por ejemplo, indicios de delito, *Represalias* asociadas o afectación a la *Alta Dirección* o al *Consejo de Administración* —, el *Responsable del Sistema Interno de Información* y *P&O* coordinarán su actuación, pudiendo la *Oficina de Compliance* retener o instruir conjuntamente la parte que corresponda.

9.4.3 Trazabilidad y protección de datos en las Comunicaciones sobre acoso

El *Responsable del Sistema Interno de Información* mantendrá el correspondiente registro en el *Libro-registro* del *Sistema*, reflejando la recepción de la *Comunicación*, su remisión y la fecha de cierre administrativo del expediente, a efectos de evidencia del funcionamiento del *Sistema*. El traspaso de información a *P&O* se realizará conforme a la normativa de protección de datos aplicable, limitándose a lo estrictamente necesario.

10. ANÁLISIS Y DECISIÓN PRELIMINAR SOBRE LA COMUNICACIÓN RECIBIDA

10.1 Análisis preliminar de la comunicación recibida

Recibida la *Comunicación* y acusado su recibo al *Informante*, el *Responsable del Sistema Interno de Información* realizará un análisis preliminar para verificar la entidad de la información, la suficiencia y verosimilitud de la misma, la credibilidad del *Informante* y la relevancia de los hechos reportados, determinando si los mismos pueden ser constitutivos de alguna infracción del Derecho de la Unión Europea, infracción penal, cuasi penal o administrativa grave o muy grave, o de algún *Incumplimiento* de la normativa interna.

Para dicho análisis preliminar, así como para las demás fases que se definen a continuación, el *Responsable del Sistema Interno de Información* podrá solicitar el asesoramiento de cualquier departamento interno que se considere oportuno, así como de *Terceros* expertos externos en la materia, en función de la complejidad fáctica o jurídica de la *Comunicación* recibida.

10.2 Decisión preliminar sobre la información recibida

En función del resultado que ofrezca el análisis preliminar, el *Responsable del Sistema Interno de Información* adoptará, levantando acta motivada, alguna de las siguientes decisiones, dentro de los diez (10) días hábiles siguientes al acuse de recibo:

a. **Inadmisión de la *Comunicación* y archivo** inmediato del expediente en los siguientes supuestos:

   - Cuando los hechos reportados no constituyan ninguno de los supuestos a los que se refiere el ámbito material de aplicación del *Sistema Interno de Información* – definido en el apartado "*Ámbito material de aplicación*" de la *Política Corporativa del Sistema Interno de Información*–.

   - Cuando la *Comunicación* sea una mera reproducción de otra anterior previamente inadmitida o debidamente investigada, sin que se aporte información nueva.

   - Cuando el contenido de la *Comunicación* resulte manifiestamente irrelevante o los hechos reportados resulten inverosímiles.

   - Cuando la información sea insuficiente para proceder con cualquier actuación adicional.

b. **Admisión de la *Comunicación* e incoación del correspondiente expediente** de investigación en relación con los hechos comunicados, conforme a lo dispuesto en el presente *Procedimiento* y los Anexos locales.

c. **Remitir con carácter inmediato la información al Ministerio Fiscal o al organismo competente en cada país** cuando los hechos comunicados pudieran ser indiciariamente constitutivos de delito o a la **Fiscalía Europea** en el caso de que los hechos afecten a los intereses financieros de la Unión Europea.

d. **Delegación del tratamiento de la *Comunicación*** a otras áreas de la *Organización* que tengan la potestad de tratar ciertos asuntos concretos, tales como aquellos relacionados con asuntos laborales al área de *P&O*.

En todos los supuestos anteriormente descritos, el *Responsable del Sistema Interno de Información* enviará *Notificación* al *Informante* sobre la inadmisión o admisión de la *Comunicación*, así como de cualquier medida adicional que se hubiera adoptado, dentro de los cinco (5) días hábiles siguientes a la conclusión del análisis preliminar, salvo que la *Comunicación* fuera anónima o el *Informante* hubiera renunciado a recibir *Notificaciones*.

10.3 Medidas cautelares

Paralelamente a la adopción de las decisiones descritas en el apartado anterior, el *Responsable del Sistema Interno de Información* podrá adoptar, en coordinación con el Departamento de *P&O* cuando resulte procedente y siguiendo el procedimiento establecido en la normativa laboral local de aplicación, todas las medidas que a la vista del *Incumplimiento* reportado se consideren necesarias para reforzar el *Sistema de Gestión de Compliance penal* de *Grupo Persán*, para el buen fin de la futura investigación y/o para la protección efectiva del *Informante*.

11. PROCEDIMIENTO DE INVESTIGACIÓN INTERNA

Cuando se opte, atendiendo a lo contemplado en el apartado 10.2.b), por iniciar un procedimiento de investigación, se deberá proceder de la siguiente forma:

- Elegir la estrategia de investigación (ver apartado 11.1).
- Planificar la investigación (ver apartado 11.2).
- Comunicación a los sujetos afectados (ver apartado 11.3).
- Realizar la propia investigación (ver apartado 11.4).
- Documentar el procedimiento de la investigación (ver apartado 11.5).
- Realizar el informe final (ver apartado 11.6).
- Actuaciones finales (ver apartado 11.7).

11.1 Elección de la estrategia de investigación

En función del ámbito, alcance y personas presuntamente involucradas en el *Incumplimiento* de que se trate, el *Responsable del Sistema Interno de Información* valorará la estrategia de investigación a desarrollar para el caso concreto, pudiendo optar por una de las siguientes opciones:

a. El procedimiento de investigación será liderado y gestionado por uno de los *Miembros de la Oficina de Compliance* o *Delegado Local*, designado por el *Responsable del Sistema Interno de Información*, sin perjuicio de las consultas o apoyo puntual que pueda requerir de otros departamentos para su completa sustanciación. Estos departamentos quedan expresamente obligados a facilitar al *Responsable del Sistema Interno de Información* cuanta información les fuere requerida y obre en su poder o conocimiento.

b. El procedimiento de investigación podrá apoyarse en un órgano o departamento interno específico de la *Organización,* cuando ello resulte recomendable por razón de su especialidad o de los conocimientos específicos necesarios para la investigación.

c. El procedimiento de investigación podrá desarrollarse con el asesoramiento de un *Tercero* experto. La elección de dicha estrategia será especialmente recomendable en los casos en los que se considere que la investigación puede requerir un especial nivel de complejidad y/o de confidencialidad.

En caso de existir algún tipo de *Conflicto de interés* en alguno de los miembros del equipo específico designado para la investigación, éste deberá apartarse de dicha investigación y no podrá intervenir en la misma.

Todas las personas que participen de manera activa en la investigación tendrán la obligación de guardar expresa reserva y confidencialidad con los hechos, datos o nombres que conozcan a raíz de la investigación.

11.2 Planificación de la investigación

Tanto el *Miembro de la Oficina de Compliance* o *Delegado Local*, en su caso, designado, planificarán la investigación con el objetivo de esclarecer los hechos ocurridos e identificar a sus responsables. Dicha planificación podrá comprender los siguientes elementos:

a. Identificar la legislación, políticas, procedimientos o normativa interna afectados, así como los *Riesgos penales o de Compliance* que pudieran derivarse del *Incumplimiento*.

b. Identificar toda la información y documentos que puedan ser relevantes y cuya revisión se considere de utilidad (correos electrónicos, sitios web, soportes audiovisuales de vigilancia y seguridad de la entidad, listas de asistentes, contraseñas o dispositivos electrónicos de seguridad, soportes contables, etc.).

   La *Oficina de Compliance* o, en su caso, el *Delegado Local* se reserva expresamente el derecho de adoptar las medidas de vigilancia y control necesarias sobre las herramientas y medios informáticos que la *Organización* pone a disposición de todos los *Miembros de la Organización*. En el supuesto de acceder a cualquier documento que pueda contener contenido personal pero el mismo se encuentre en soportes y/o equipos profesionales, el acceso deberá hacerse de forma prudente atendiendo (siempre atendiendo al juicio de idoneidad, necesidad, utilidad y proporcionalidad) y garantizando la cadena de custodia.

c. Determinar, en el caso de que fuese necesario, de forma suficientemente motivada y, con la colaboración del Departamento de *P&O*, la necesidad y, en su caso, la urgencia de adoptar medidas cautelares con respecto a los sujetos afectados por la *Comunicación*. Las medidas cautelares no están limitadas, pero pueden incluir las siguientes:

   - Trasladar a los sujetos investigados a otra división, área o departamento o cambiarlos de ubicación de manera temporal.

   - Modificar las tareas o responsabilidades habituales de los sujetos afectados por la *Comunicación*.

   - Suspender de empleo y sueldo a los sujetos afectados por la *Comunicación* de manera inmediata.

d. Definir los pasos a seguir en la investigación y en las diferentes reuniones con los afectados con el objetivo de velar por su correcto desarrollo, identificando interlocutores a entrevistar, preguntas relevantes a realizar, posibles testigos del hecho comunicado, entre otros.

e. Incluir en el expediente de investigación toda la información que pueda resultar de interés en relación con la vida laboral del sujeto afectado en *Grupo Persán* (historial de empleo, contingencias anteriores, políticas, procedimientos y normativa de la *Organización* que le resulten de especial aplicabilidad, etc.).

f. Al planificar la investigación se tratará siempre de favorecer:

   - La objetividad y equidad del proceso;

   - La privacidad de los sujetos investigados; y

   - La minimización del impacto de la investigación.

Cuidando siempre de cumplir con los principios que rigen el *Sistema Interno de Información* establecidos en la *Política Corporativa del Sistema Interno de Información*.

11.3 Comunicación a los sujetos afectados

Con carácter previo a iniciar la investigación, el *Miembro de la Oficina de Compliance* designado o *Delegado Local* (en adelante, el ***"investigador"***) se pondrá en contacto con los sujetos *Denunciados*, identificándose ante éstos como encargado de la investigación de la posible irregularidad o infracción comunicada, informándoles acerca de los hechos que se les atribuyen y de los principales hitos que se pueden producir durante la investigación.

Adicionalmente el *Denunciado* será informado del derecho que tiene a presentar alegaciones por escrito y del tratamiento de sus datos personales, su derecho a ser oída en cualquier momento y demás derechos que les asisten recogidos en la *Normativa de Protección al Informante* y la *Política Corporativa del Sistema Interno de Información*.

Lo anterior se llevará a cabo, salvo que, a juicio del investigador, y para evitar que puedan destruirse y/u ocultarse pruebas, o de otro modo, perjudicar a la propia investigación, se deba realizar la *Notificación* al *Denunciado* en un momento posterior y, en todo caso, cuando se requiera la declaración de este, en el momento del trámite de audiencia o antes de finalizar el proceso de investigación.

En ningún caso se comunicará a los sujetos afectados por la *Denuncia* la identidad del *Informante* ni se dará acceso a la *Comunicación*.

Sin perjuicio del derecho a formular alegaciones por escrito, la investigación comprenderá, siempre que sea posible, una entrevista con el *Denunciado* en la que, siempre con absoluto respeto a la presunción de inocencia, se le invitará a exponer su versión de los hechos y a aportar aquellos medios de prueba que considere adecuados y pertinentes.

11.4 Desarrollo de la investigación

La investigación incluirá todas aquellas diligencias de investigación que resulten oportunas para el esclarecimiento de los hechos, las personas responsables y las medidas correctoras que deban en su caso adoptarse.

En cualquier caso, la investigación se llevará a cabo siempre con el máximo respeto a los principios que rigen el *Sistema Interno de Información* recogidos en el apartado "*Principios básicos del Sistema Interno de Información*" de la *Política* y, en especial, en relación con el deber de confidencialidad y protección del *Informante* y respetando en todo caso la presunción de inocencia, el derecho a ser oído y el derecho al honor del *Denunciado*.

Se detallan a continuación algunas de las principales diligencias que podrán conformar la investigación:

a. Celebración de una entrevista con el *Informante* a fin de obtener más información sobre la *Comunicación* presentada.

b. Declaración de los sujetos afectados por la *Comunicación*.

c. Realizar cuestionarios y entrevistas con testigos.

d. Concertar audiencias con los superiores y compañeros de los *Denunciados*, así como, con cualesquiera personas que se considere necesarias.

e. Recabar cuanta información sea posible a través de la documentación de *Grupo Persán*.

f. Si fuera indispensable para el esclarecimiento de los hechos, adoptar medidas de vigilancia a través de detectives o medios informáticos, telemáticos o audiovisuales, siempre que los mismos atiendan a criterios de razonabilidad, idoneidad y proporcionalidad, velando en todo momento por el derecho a la intimidad del *Miembro de la Organización* y por el derecho al secreto de las comunicaciones, así como cualquier otra normativa local vigente en esta materia.

g. Solicitar ayuda externa de otros profesionales.

h. Cualesquiera otras diligencias que el *Responsable del Sistema Interno de Información* estime necesarias para el esclarecimiento de los hechos, incluyendo el potencial mantenimiento de *Notificaciones* con el *Informante* y, si se considera necesario, la solicitud de información adicional al mismo.

La duración de las actuaciones de investigación no podrá ser superior a 3 meses a contar desde la recepción de la *Comunicación*. De forma excepcional, en casos de especial complejidad que requieran una ampliación del plazo, este podrá extenderse de forma motivada hasta un máximo de otros 3 meses adicionales.

11.5 Documentación del procedimiento de investigación

Será imprescindible incluir en el expediente la documentación detallada de todo el procedimiento de investigación desarrollado, incluyendo el plan de investigación inicialmente elaborado, todos los documentos que se vayan recabando y las actas de las entrevistas que se mantengan.

Todas las entrevistas que se realicen se documentarán debidamente, bien mediante la elaboración de una transcripción completa y exacta por parte del *Responsable del Sistema Interno de Información*, que deberá ratificarse y firmarse por los comparecientes – previo ofrecimiento a los mismos para que la comprueben y rectifiquen – y por el propio *Responsable del Sistema Interno de Información*, bien mediante una grabación en un formato seguro, duradero y accesible – previa advertencia a los comparecientes de que la *Comunicación* será 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 –.

Asimismo, se procederá a informar, en todas ellas, de la recogida, tratamiento y divulgación de los datos de carácter personal de conformidad con la legislación vigente en materia de protección de datos.

11.6 Informe final

Una vez finalizadas todas las diligencias de investigación, el investigador elaborará un informe de conclusiones que deberá contener una breve descripción de los siguientes elementos:

a. **Naturaleza de la contingencia**: Se identificarán, en la medida de lo posible, los sujetos intervinientes, la naturaleza de los hechos, la fecha, el lugar y las circunstancias en que supuestamente sucedieron, los preceptos legales o la normativa interna infringida o puesta

en peligro, lo que incluirá una exposición de los hechos relatados junto con el código de identificación de la *Comunicación* y la fecha de registro.

b. **Identidad del investigador**: Se identificará debidamente a la persona o personas componentes del equipo de trabajo que hayan llevado a cabo la investigación.

c. **Clasificación de la *Comunicación*** a efectos de conocer su prioridad o no en su tramitación.

d. **Las actuaciones realizadas** con el fin de comprobar la verosimilitud de los hechos.

e. **Relación de los hechos y descubrimientos relevantes**: Se relatarán los hechos más relevantes identificados a lo largo del procedimiento de investigación, diferenciándolos, atendiendo a la fuente de información a partir de la que fueron identificados, por ejemplo:

- Documentación de *Grupo Persán*;
- Información proporcionada por el *Informante*, o;
- Información obtenida de las entrevistas mantenidas con los sujetos afectados por la *Comunicación* y con los testigos.

f. **Conclusiones y valoración de los hechos**: Se especificarán las conclusiones extraídas por el investigador y de los indicios que las sustentan, así como su valoración de los hechos relatados, pudiendo proponer dos posibles acciones:

- **Propuesta de continuación del procedimiento** si se estima que, de las diligencias practicadas, ha quedado suficientemente acreditada la comisión por parte del sujeto afectado de cualquiera de las infracciones establecidas en el apartado "*ámbito material de aplicación*" de la *Política Corporativa del Sistema Interno de Información*.
- **Archivo del procedimiento** si se estima que el hecho no es constitutivo de las infracciones referidas en el apartado "*ámbito material de aplicación*" de la *Política Corporativa del Sistema Interno de Información*, no está suficientemente justificada su perpetración o no se ha podido conocer su autor. El archivo del procedimiento será comunicado al *Informante* y, en su caso, a la persona afectada por la *Comunicación*.

11.7 Actuaciones finales

Una vez elaborado el informe final de investigación será inmediatamente, a lo largo de la jornada, trasladado al *Responsable del Sistema Interno de Información*.

El informe final de investigación deberá quedar archivado junto con el resto del expediente de investigación.

12. CONCLUSIÓN DEL PROCEDIMIENTO

12.1 Órgano responsable

Corresponde al *Responsable del Sistema Interno de Información* resolver, a la vista de la propuesta contenida en el informe final del investigador, y adoptar alguna de las decisiones previstas en el apartado 12.3 del presente *Procedimiento*.

Cuando la persona *Denunciada* sea un *Miembro de la Oficina de Compliance* o el *Delegado Local*, dicha persona deberá abstenerse de intervenir en la valoración y resolución del expediente que le afecte.

12.2 Trámite de audiencia

Una vez recibido el informe final de investigación, el *Responsable del Sistema Interno de Información* informará a los *Denunciados* del resultado de la investigación, a quien se concederá un plazo razonable para alegar por escrito, o mediante entrevista, lo que considere pertinente.

En la *Notificación* al *Denunciado* del informe final deberá omitirse cualquier información sobre la naturaleza del procedimiento seguido, de los hechos o de las medidas adoptadas que pueda revelar la identidad del *Informante* o pueda infringir la *Normativa de protección al Informante* y/o la normativa reguladora de la protección de datos personales.

12.3 Decisiones del Responsable del Sistema Interno de Información

Una vez transcurrido el plazo para que el *Denunciado* formule sus alegaciones, se podrán adoptar alguna de las siguientes decisiones:

a. **Admitir o inadmitir las pruebas interesadas por el *Denunciado***, de forma motivada.

b. **Solicitar la práctica de diligencias de investigación adicionales** al investigador.

c. **Archivar el expediente** por ausencia de prueba suficiente o por carecer los hechos de relevancia a estos efectos, procediéndose al archivo.

d. **Declarar la comisión de un *Incumplimiento* en *Grupo Persán*** y proponer, en su caso, la sanción o medida al Departamento de *P&O*, órgano competente para su imposición.

e. Cuando, tras la emisión del informe final se determine que los hechos pudieran ser indiciariamente constitutivos de delito, la información obtenida en **la investigación será remitida al Ministerio Fiscal o al organismo competente en cada país** con carácter inmediato. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá dicha información a la Fiscalía Europea.

12.4 Sanciones

Las sanciones que podrán imponerse a los *Miembros de la Organización* en cada caso serán las previstas en los Convenios Colectivos de aplicación (o en su caso, documentos equivalentes) o en la legislación laboral aplicable en cada jurisdicción.

Tales sanciones se graduarán atendiendo a la gravedad de los hechos cometidos, pudiendo tomarse en consideración circunstancias tales como la reincidencia, el daño o perjuicios causados, las circunstancias de las víctimas, si las hubiere, entre otras.

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.

La aplicación de estas sanciones se canalizará a través del Departamento de *P&O*.

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 el presente *Procedimiento* y sus Anexos locales, los cuales, incluyen entre otras, el cese de las relaciones de negocio.

12.5 Otras medidas

Se podrán adoptar otras medidas adicionales de reacción y respuesta, tales como, a efectos enunciativos, pero no limitativos:

a. Reportar los hechos a cualquier autoridad con competencia sobre los mismos, bien sea administrativa o judicial.

b. Evaluar indicios anteriores de infracciones similares y asegurar la toma de medidas adecuadas para comprender la causa del *Incumplimiento*.

c. Adoptar acciones resarcitorias respecto de cualquier persona o entidad que pudiera haber resultado perjudicada por los hechos.

d. Establecer procesos, procedimientos y controles para evitar la comisión de *Incumplimientos* similares y proponer medidas organizativas o de prevención de cualquier clase.

e. Tomar decisiones relacionadas con la *Comunicación*, formación o difusión interna de los hechos, tanto a nivel de órgano o unidad (división, área o departamento) de *Grupo Persán*, como a nivel general (al conjunto de los *Miembros de la Organización*) cuando ello se considere una herramienta eficaz para prevenir *Incumplimientos* similares en el futuro (siempre con las debidas cautelas en materia de Protección de Datos de Carácter Personal).

12.6 Comunicación de las decisiones

Las decisiones adoptadas una vez concluida la investigación interna se notificarán inmediatamente y por escrito a los sujetos afectados, así como al *Informante*. En la *Notificación* a los *Denunciados* o a los *Denunciantes* podrá omitirse cualquier información sobre la naturaleza del procedimiento seguido, de los hechos o de las medidas adoptadas, en orden a dar cumplimiento a la normativa reguladora de la protección de datos personales y a los principios establecidos en este *Procedimiento* y la *Política Corporativa del Sistema Interno de Información*.

13. CONSERVACIÓN DE LA DOCUMENTACIÓN

13.1 Plazos de conservación

Los datos personales recabados a través del *Sistema Interno de Información* se conservarán de conformidad con lo dispuesto en la legislación local aplicable. En concreto, 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 *Grupo Persán*.

13.2 Registro de comunicaciones

Grupo Persán llevará un registro de todas las *Denuncias* y *Consultas* que pueda recibir a través del *Sistema Interno de Información*, recopiladas en el llamado "***Libro-registro***", gestionado a través de la plataforma EQS, 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.

El *Responsable del Sistema Interno de Información* registrará las *Comunicaciones* recibidas, incluyendo la siguiente información:

- Fecha de recepción.
- Número de expediente.
- Fecha en la que termina el plazo máximo de investigación de tres (3) meses.
- Medio o canal de recepción de la *Comunicación*.
- Identidad del *Informante* o, en su caso, indicación de que se trata de una *Comunicación* anónima.
- Identidad del *Denunciado* o *Denunciados* por la *Comunicación*.

Asimismo, el *Responsable del Sistema Interno de Información* registrará las actuaciones e investigaciones realizadas en cada expediente, incluyendo la siguiente información:

- Acuse de recibo de la *Comunicación*.
- Inadmisión/admisión de la *Comunicación*.
- Notificación al *Informante* de la admisión o inadmisión de la *Comunicación*.
- En caso de solicitud, reunión con el *Informante* en el plazo máximo de siete (7) días naturales.
- En su caso, solicitud de información adicional al *Informante*.

- Notificación al *Denunciado* de los hechos que se le atribuyen y de sus derechos.
- Audiencia con el *Denunciado*.
- Diligencias de investigación practicadas.
- Emisión por el *Responsable del Sistema Interno de Información* del informe final con la propuesta de resolución.
- Notificación del informe final a la persona/s *Denunciada/s*.
- Decisión final del *Responsable del Sistema Interno de Información*.
- En su caso, comunicación a las autoridades competentes en caso de que los hechos sean constitutivos de delito.
- Otras actuaciones.

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

1. Mediante una grabación de la conversación en un formato duradero y accesible.
2. 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. *Grupo 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.

Únicamente a petición razonada de la Autoridad judicial competente, mediante auto, y siempre en el marco de un procedimiento judicial y bajo la tutela de aquella, podrá accederse total o parcialmente al contenido del *Libro-registro*.

Los datos contenidos en este *Libro-registro* se conservarán únicamente durante el tiempo que sea necesario y, en todo caso, no podrán conservarse por un periodo superior a diez (10) años, salvo cuando para el adecuado ejercicio del derecho a la defensa pueda ser necesario el mantenimiento de los datos por un plazo superior.

El citado *Libro-registro* así como los tratamientos realizados por los intervinientes en la tramitación de las *Comunicaciones* recibidas a través del *Canal Ético*, cumplirá con las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad de los datos personales adecuado al riesgo y, en su caso, aquellas previstas por la normativa sobre protección de datos que resulte de aplicación.

14. PROTECCIÓN DE DATOS PERSONALES

14.1 PRINCIPIOS GENERALES

Grupo Persán garantiza el tratamiento de los datos personales obtenidos a través del *Canal Ético* de conformidad con lo dispuesto en el Reglamento (UE) 2016/679 (RGPD), la normativa nacional de protección de datos aplicable en cada jurisdicción donde opere la *Organización* y la correspondiente *Normativa de Protección al Informante.*

El tratamiento de los datos personales se realizará observando en todo momento los principios de licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, integridad, confidencialidad y responsabilidad proactiva.

14.2 RESPONSABLES DEL TRATAMIENTO

En el marco de la gestión de las *Comunicaciones* recibidas a través del *Sistema Interno de Información*, tendrán la condición de responsables del tratamiento:

- La sociedad de *Grupo Persán* con la que el *Informante*, las *Personas afectadas* por la *Denuncia* o cualquier otra persona implicada mantenga una relación laboral, mercantil, contractual o profesional.

- PERSÁN, S.A., como entidad matriz de *Grupo Persán*, cuando participe en la supervisión, coordinación, gestión o investigación de las *Comunicaciones* a través de la *Oficina de Compliance*, o el *Responsable del Sistema Interno de Información*.

14.3 CATEGORÍAS DE DATOS TRATADOS

En el marco de la recepción, análisis, investigación y resolución de las *Comunicaciones* podrán tratarse las siguientes categorías de datos personales:

- Datos identificativos y de contacto del *Informante*, *Persona afectada* o *Terceros* relacionadas con los hechos comunicados, tales como nombre y apellidos, dirección postal, dirección de correo electrónico, teléfono.

- Datos profesionales, laborales o de negocio, incluyendo puesto de trabajo, función o relación con el *Grupo Persán.*

- Presuntos *Incumplimientos* comunicados.

- Documentación que pruebe los presuntos *Incumplimientos* sobre los que se informa.

Únicamente serán tratados aquellos datos que resulten adecuados, pertinentes y limitados a lo necesario para el cumplimiento de las finalidades previstas en este *Procedimiento GIR*.

14.4 FINALIDADES DEL TRATAMIENTO Y BASES LEGITIMADORAS

Los datos personales serán tratados con las siguientes finalidades:

- Recibir, registrar, gestionar y dar respuesta a las *Comunicaciones* presentadas a través del *Sistema Interno de Información.*

- Analizar, verificar e investigar posibles *Incumplimientos.*

- Proteger a los *Informantes* y garantizar la efectividad de las medidas previstas en la *Normativa de Protección al Informante.*

- Gestionar la adopción de medidas disciplinarias, correctivas, organizativas, administrativas, judiciales o de cualquier otra naturaleza que resulten procedentes.

- Garantizar el adecuado funcionamiento del *Sistema Interno de Información*.

Por tanto, las bases de legitimación para el tratamiento de los datos personales serán, según corresponda en cada caso:

- El cumplimiento de una obligación legal en aquellos casos en los que exista una normativa en la que se exija la necesidad de disponer de un sistema que permita la comunicación a las personas que trabajan para una entidad privada sobre asuntos de los que tengan conocimiento relativos a posibles infracciones normativas y de lucha contra la corrupción.

- El interés público en aquellos casos en los que no exista una normativa específica que regule la necesidad de crear un sistema interno de información o canal de denuncias y sea necesario realizar un tratamiento de datos personales para prevenir y actuar frente a posibles infracciones normativas y de lucha contra la corrupción.

- El interés legítimo que tiene el *Grupo Persán* en perseguir y prevenir el cumplimiento de su normativa interna.

- La ejecución y gestión de la relación laboral, profesional, mercantil o contractual existente entre el interesado y cualquiera de las entidades de *Grupo Persán* cuando resulte necesaria para la tramitación de la *Comunicación.*

14.5 CONFIDENCIALIDAD

Grupo Persán adoptará las medidas técnicas y organizativas necesarias para preservar la confidencialidad de la información recibida y proteger la identidad del Informante, de la Persona afectada por la Denuncia y de cualquier tercero mencionado en una Comunicación.

El acceso a la identidad del Informante quedará estrictamente limitado a las personas autorizadas para la gestión del Sistema Interno de Información y únicamente podrá revelarse en los supuestos legalmente exigibles y de conformidad con las garantías previstas en la normativa aplicable.

Las *Personas afectadas* por una *Denuncia* serán informadas sobre el tratamiento de sus datos personales y sobre los hechos que les conciernan en los términos previstos por la legislación aplicable, siempre que dicha información no comprometa la investigación ni la protección del *Informante*. En cualquier caso, el ejercicio del derecho de acceso de la *Persona afectada* estará limitado a sus propios datos de carácter personal, sin que se puedan entender incluidos dentro del ejercicio de ese derecho los datos personales relativos al *Informante*. Así mismo, el derecho de oposición también se encuentra limitado con carácter general por entenderse que existen motivos legítimos imperiosos que legitiman el tratamiento de los datos personales.

14.6 CONSERVACIÓN DE LOS DATOS

Los datos personales tratados en el *Sistema Interno de Información* serán conservados únicamente durante el tiempo necesario para cumplir la finalidad para la que fueron recabados y para atender las obligaciones legales aplicables.

Con carácter general, los datos de carácter personal obtenidos en el marco de la investigación interna serán suprimidos cuando dejen de ser necesarios y pertinentes y, en todo caso, en el plazo máximo de tres (3) meses desde que se registre la *Comunicación*, salvo que la investigación siga en curso o en los casos en los que la finalidad sea evidenciar el funcionamiento del *Sistema*, en cuyo caso se mantendrán anonimizados.

Los datos personales que no tengan cabida en el ámbito de aplicación del *Canal Ético*, no sean necesarios para el desarrollo de la investigación y/o no sean objeto de investigación, o cuando se acredite que la información no es veraz, se suprimirán o serán anonimizados, salvo en los casos previstos por la normativa que resulte de aplicación.

14.7 DESTINATARIOS DE LOS DATOS

Para cumplir con las finalidades del tratamiento mencionadas, los datos personales podrán ser comunicados o resultar accesibles exclusivamente a aquellas personas y entidades cuya intervención sea necesaria para la adecuada gestión de la *Comunicación*, incluyendo:

- El *Responsable del Sistema Interno de Información*.
- Los Delegados Locales debidamente autorizados.
- La *Oficina de Compliance*.
- Aquellas áreas/departamentos/entidades del *Grupo Persán* relevantes de cara a la investigación y las posibles medidas a tomar con respecto a la conducta comunicada en cuestión.
- Los órganos de dirección o gobierno de *Grupo Persán* cuando resulte necesario.
- Asesores externos, profesionales o proveedores especializados que colaboren en la gestión o investigación de una Comunicación.
- Autoridades judiciales, administrativas, fiscales, policiales o reguladoras competentes.

Todos los destinatarios estarán sujetos a las correspondientes obligaciones de confidencialidad y protección de datos.

14.8 TRANSFERENCIAS INTERNACIONALES DE DATOS

Algunas de las entidades tanto del *Grupo Persán* como proveedores de servicios, pueden encontrarse ubicadas fuera del Espacio Económico Europeo y, por tanto, no proporcionar un nivel de protección de datos equiparable al de la Unión Europea.

En tales casos, *Grupo Persán* adoptará las garantías adecuadas exigidas por la normativa aplicable relativa a la transferencia internacional de datos, tales como las Cláusulas Contractuales Tipo o cualquier otra medida complementaria pertinente. Puede consultarse el contenido de las Cláusulas

Contractuales Tipo en el siguiente enlace: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en.

14.9 DERECHOS DE LOS INTERESADOS

Por último, bajo las condiciones que se establecen en la normativa aplicable, se podrán ejercitar los siguientes derechos:

- **Derecho de acceso**: tiene derecho a solicitar de la *Organización* que confirme si está tratando sus datos personales y, en caso afirmativo, a solicitar el acceso a los mismos. Los datos de acceso incluyen – entre otros – las finalidades del tratamiento, las categorías de los datos personales afectados, y los destinatarios o las categorías de destinatarios a los que los datos personales han sido o serán comunicados. Podrá obtener una copia de los datos personales que estén siendo objeto de tratamiento.

- **Derecho de rectificación**: tiene derecho a solicitar a la *Organización* que rectifique los datos personales incorrectos o incompletos.

- **Derecho de supresión (derecho al olvido):** tiene derecho a solicitar la *Organización* que elimine sus datos personales.

- **Derecho de limitación del tratamiento:** tiene derecho a solicitar la limitación del tratamiento de sus datos personales, si bien la *Organización* llevará a cabo un análisis caso por caso para determinar si efectivamente procede el ejercicio de dicho derecho.

- **Derecho de oposición:** cuando se cumplan determinadas circunstancias, tendrá derecho a oponerse al tratamiento que realizamos de sus datos personales.

Los interesados podrán ejercitar sus derechos mediante el envío de un correo electrónico a la dirección gdpr@persan.es o la dirección postal de PERSÁN, S.A, esto es, C/ Pino Albar, 2, 41.016. Sevilla, con la referencia "**Protección de Datos**" identificando el derecho que desean ejercitar. Asimismo, tendrán el derecho a presentar una reclamación ante la autoridad de protección de datos competente en cada caso.

15. DIFUSIÓN, REVISIÓN Y ACTUALIZACIÓN DEL PROCEDIMIENTO

El presente *Procedimiento* estará a disposición de todos los *Miembros de la Organización* a través de los canales internos de comunicación corporativa que resulten adecuados en cada momento. Asimismo, se pone a disposición *Socios de negocio*, *Terceros* y demás grupos de interés mediante la página web corporativa o a través de otros medios que la *Organización* considere oportunos en determinadas circunstancias para garantizar su adecuada difusión y conocimiento.

Con el fin de asegurar su correcta aplicación, la *Organización* impulsará las acciones de comunicación, formación y sensibilización que resulten necesarias para favorecer el conocimiento, comprensión y cumplimiento de las disposiciones contenidas en este *Procedimiento* por parte de sus destinatarios.

El presente *Procedimiento* será objeto de revisión periódica y podrá ser actualizado cuando resulte necesario, a propuesta de la *Oficina de Compliance*, con la finalidad de garantizar su adecuación a las modificaciones normativas que resulten aplicables, a la evolución de las mejores prácticas en la materia y a los cambios que puedan producirse en la actividad, organización o entorno de actuación del *Grupo Persán*.

Cualquier actualización será debidamente comunicada a las personas destinatarias, adoptándose las medidas oportunas para asegurar su efectiva implantación y cumplimiento.