WHISTLEBLOWING AND OTHER REPORTING

PROCEDURE

CODE	REV	DATE OF ISSUE	CLASSIFICATION
PO.SGI.10	00	13/11/2026	PUBLIC

Índice

1. Introducción 3
1.1 Matriz de redacción y revisiones 3
1.2 Objeto y ámbito de aplicación 4
1.2.1 Objeto 4
1.2.2 Ámbito de aplicación 4
1.3 Referencias normativas y documentales 4
1.4 Definiciones y abreviaturas 4
1.4.1 Definiciones 4
1.4.2 Abreviaturas 5
1.5 Responsabilidades 5
2. Modalidades operativas 6
2.1 Introducción 6
2.1.1 Principios generales 6
2.2 Tipos de comunicaciones 6
2.2.1 Comunicaciones internas 7
2.2.2 Comunicaciones externas 7
2.2.3 Revelación pública 8
2.2.4 Denuncia ante la Autoridad Judicial o el Tribunal de Cuentas 8
2.2.5 Comunicaciones realizadas de mala fe 8
2.3 El Gestor de las Comunicaciones 9
2.4 Proceso de gestión de las comunicaciones internas 9
2.4.1 Recepción 9
2.4.2 Evaluación preliminar e instrucción 10
2.4.3 Definición de las acciones consiguientes 11
2.4 Reporting y seguimiento 11
2.5 Conservación de la documentación 11
2.6 Régimen de whistleblowing y Modelo 231 11
2.7 Canal de comunicación compartido 12
2.8 Protección de datos personales 13
3. Documentación relacionada 13

1. Introducción

1.1 Matriz de redacción y revisiones

REVISION	DESCRIPTION	EDITING		VERIFICATION		APPROVAL	
		Date	**Name Signature**	**Date**	**Name Signature**	**Date**	**Name Signature**
00	Primera emisión tras el proceso de integración del SGI del grupo Medisolve.	26/10/2026	L. Scaglia	06/11/2026	R. Raimondo Avv. Roberta Raimondo	13/11/2026	N. Alloa Casale

1.2 Objeto y ámbito de aplicación

1.2.1 Objeto

El presente documento tiene por objeto definir los principios, las responsabilidades y las modalidades operativas para la gestión del proceso/actividad regulada por el procedimiento, con el fin de garantizar su aplicación coherente, controlada y conforme a los requisitos del Sistema de Gestión Integrado del Grupo Medisolve (en adelante, también, el "Grupo") y a la normativa vigente.
El procedimiento asegura la uniformidad de enfoque entre las distintas sociedades del Grupo y constituye la referencia para todas las funciones implicadas en las actividades descritas.

1.2.2 Ámbito de aplicación

El presente procedimiento se aplica a todas las sociedades pertenecientes al Grupo que hayan acordado su incorporación formal, mediante aprobación por el Consejo de Administración o por la persona formalmente delegada.

El procedimiento es eficaz y aplicable desde la fecha de emisión y es vinculante para las funciones, procesos y actividades comprendidos en el ámbito de aplicación del Sistema de Gestión de cada sociedad.

1.3 Referencias normativas y documentales

- ISO 9001, 13485, 14001, 45001, 27001, 37001, PdR125, SA8000;
- D.Lgs. 24/2023, de transposición de la Directiva (UE) 2019/1937 relativa a la protección de las personas que informen sobre infracciones (Whistleblowing)
- Código Ético y de Conducta;
- Modelo de Organización, Gestión y Control conforme al D.Lgs. 231/2001, cuando se haya adoptado;
- 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 (España);
- Real Decreto 1101/2024, de 29 de octubre, por el que se aprueba el Estatuto de la Autoridad Independiente de Protección del Informante, A.A.I. (España);
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (España);
- Artículo 31 bis de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, relativo a los modelos de organización y gestión para la prevención de delitos (España).

1.4 Definiciones y abreviaturas

1.4.1 Definiciones

- **Gestor de las Comunicaciones**: persona u órgano formalmente designado por la sociedad para la recepción y gestión de las comunicaciones.
- **Función competente**: persona encargada de la fase de instrucción y de la gestión de las eventuales acciones consiguientes.
- **Comunicación**: transmisión, escrita u oral, de información sobre infracciones.
- **Comunicación de Whistleblowing**: comunicación que tiene por objeto información sobre infracciones, reales o potenciales, de disposiciones normativas nacionales o de la Unión Europea, del Código Ético o de otras disposiciones cuya comunicación esté protegida por la

normativa aplicable en materia de whistleblowing. Estas comunicaciones gozan de las medidas de protección específicas previstas por la ley.

- **Otra Comunicación**: comunicación relativa a observaciones, reclamaciones, sugerencias, solicitudes de aclaración, no conformidades, incidencias operativas u otros hechos de interés para la organización que no entran en el ámbito de las comunicaciones de whistleblowing, pero que requieren una evaluación y gestión por parte de las funciones competentes.
- **Whistleblowing**: se entiende por tal la protección de las personas que informan sobre infracciones de disposiciones normativas nacionales o de la UE.
- **Sistema interno de información (España):** conjunto formado por el canal o canales internos, el Responsable del Sistema y el procedimiento de gestión de informaciones que las Entidades en España deben implantar conforme a la Ley 2/2023.
- **Responsable del Sistema (España):** persona física u órgano colegiado designado por el órgano de administración de la Entidad en España como responsable de la gestión del Sistema interno de información (art. 8 de la Ley 2/2023). Para las Entidades en España, las funciones atribuidas en el presente procedimiento al Gestor de las Comunicaciones se ejercerán por el Responsable del Sistema o bajo su supervisión.
- **Informante (España):** persona física que comunica información sobre infracciones obtenida en un contexto laboral o profesional, incluidos, entre otros, trabajadores por cuenta ajena, autónomos, accionistas, partícipes y miembros del órgano de administración, dirección o supervisión, personas que trabajen para o bajo la supervisión de contratistas, subcontratistas y proveedores, así como voluntarios, becarios, trabajadores en formación, candidatos en procesos de selección y personas cuya relación laboral o estatutaria haya finalizado (art. 3 de la Ley 2/2023).
- **Persona afectada (España):** persona física o jurídica a la que se atribuyen las acciones u omisiones objeto de la comunicación.

1.4.2 Abreviaturas

- ANAC: Autorità Nazionale Anticorruzione (Autoridad Nacional Anticorrupción italiana)
- A.A.I.: Autoridad Independiente de Protección del Informante (España)
- LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

1.5 Responsabilidades

Todas las funciones y personas implicadas en las actividades reguladas por el presente procedimiento están obligadas a aplicarlo conforme a los requisitos definidos por el Sistema de Gestión Integrado del Grupo y por la normativa vigente.

2. Modalidades operativas

2.1 Introducción

El presente procedimiento define los principios, las modalidades generales y las responsabilidades para la gestión de las comunicaciones recibidas por las sociedades del Grupo.
El objetivo es garantizar un proceso uniforme, transparente, imparcial y confidencial para la recepción, evaluación y gestión de las comunicaciones procedentes de las partes interesadas, conforme a la normativa aplicable y a los principios éticos adoptados por el Grupo.
Cada sociedad mantiene, además, la responsabilidad de la gestión de las comunicaciones de su competencia, salvo las centralizaciones que el Grupo haya definido formalmente.

2.1.1 Principios generales

La gestión de las comunicaciones se basa en los siguientes principios:

Confidencialidad
La identidad de las personas implicadas y la información contenida en las comunicaciones se tratan conforme a las disposiciones aplicables y con criterios de estricta confidencialidad.

Imparcialidad
Cada comunicación se gestiona de forma objetiva, independiente y libre de prejuicios o conflictos de interés.

Buena fe
Las comunicaciones deben presentarse de buena fe y sobre la base de elementos que el informante considere razonablemente fundados.

Protección de las personas afectadas
Se garantizan el respeto de los derechos de las personas interesadas y la correcta gestión de la información recabada durante el proceso de evaluación.

Prohibición de represalias
El Grupo no tolera comportamientos de represalia o discriminatorios contra las personas que realizan comunicaciones de buena fe.

Protección de datos personales
Los datos personales obtenidos durante la gestión de las comunicaciones se tratan conforme a la normativa aplicable.

2.2 Tipos de comunicaciones

Las sociedades del Grupo pueden recibir tanto comunicaciones de whistleblowing, sujetas a las garantías previstas por la normativa aplicable, como otras comunicaciones relativas a actividades, procesos, productos, servicios o comportamientos de la empresa.
Las comunicaciones se distinguen, además, en función del canal utilizado; así, tenemos:

- Comunicaciones internas, que utilizan canales de comunicación internos
- Comunicaciones externas, que utilizan canales de comunicación externos
- Revelaciones públicas
- Denuncia ante la autoridad judicial

2.2.1 Comunicaciones internas

Las sociedades del Grupo ponen a disposición canales de comunicación específicos, idóneos para garantizar niveles adecuados de seguridad, confidencialidad y trazabilidad.
La principal herramienta para el envío y la gestión de las comunicaciones son los "Portales de Comunicación", también denominados "portales de whistleblowing", que, en su caso, adopte cada sociedad del Grupo y a los que se accede directamente mediante un enlace desde sus respectivos sitios web. Cada portal, cuando sea necesario, ofrece instrucciones adicionales sobre su funcionamiento.
Las comunicaciones recibidas a través de estos canales podrán considerarse comunicaciones de whistleblowing cuando entren en el ámbito definido por la norma; para más detalles al respecto, se remite a la política correspondiente **PL.PO.SGI.10-01**.
A través de estos portales también pueden enviarse otras comunicaciones que, aunque no entren en el perímetro de las comunicaciones de whistleblowing, pueden beneficiarse, mediante el uso del canal específico, del completo anonimato y de un flujo de gestión formalizado.
Además de los portales, es posible enviar comunicaciones internas a través de direcciones de correo electrónico específicas. En cuanto al funcionamiento de estos canales, se remite a lo indicado en los distintos procedimientos del Grupo (se precisa que, aunque el Grupo garantiza en estos canales el respeto de los principios básicos, estos no quedan comprendidos en la protección prevista por el Whistleblowing).
Para las Entidades en España, todos los canales internos, incluidos los buzones de correo electrónico, se integran en el Sistema interno de información y permiten comunicar por escrito o verbalmente, incluida una reunión presencial a solicitud del informante en un plazo máximo de siete días. Las comunicaciones verbales se documentan, con el consentimiento del informante, mediante grabación o transcripción que este podrá revisar y firmar (arts. 5 y 7 de la Ley 2/2023).
Quien reciba una comunicación por un canal distinto deberá mantener su confidencialidad y remitirla de inmediato al Responsable del Sistema. La información sobre el canal interno y los canales externos se publicará en la página de inicio de la web, en una sección separada y fácilmente identificable (arts. 9 y 25 de la Ley 2/2023).

2.2.2 Comunicaciones externas

El canal externo constituye una herramienta alternativa a los canales internos de la empresa y solo puede utilizarse en los casos y en las condiciones previstos por la normativa vigente.
El Grupo fomenta, cuando sea posible y apropiado, el uso preferente de los canales internos para permitir una gestión tempestiva de las cuestiones comunicadas.
Para las Entidades en España, el canal externo es el gestionado por la Autoridad Independiente de Protección del Informante, A.A.I., cuando la infracción afecte o produzca sus efectos en el ámbito territorial de más de una comunidad autónoma, o por las autoridades u órganos autonómicos competentes cuando la infracción se circunscriba al ámbito territorial de la correspondiente comunidad autónoma. La norma permite al informante dirigirse al canal externo directamente o tras haber utilizado el canal interno, sin necesidad de que concurra ninguna condición previa.

2.2.2.1 Información útil sobre el canal de la ANAC

Conforme a la normativa aplicable en materia de whistleblowing, el informante puede realizar una comunicación a través del canal externo establecido y gestionado por la ANAC.
Las modalidades operativas, los requisitos de admisibilidad y las garantías aplicables están regulados directamente por la ANAC y pueden consultarse en su sitio web institucional.
El canal de la ANAC puede utilizarse cuando concurra al menos una de las siguientes condiciones previstas por el D.Lgs. 24/2023:

- el canal interno no está previsto o no es conforme;
- el informante ya ha realizado una comunicación interna sin que se le haya dado seguimiento;
- existe un temor fundado de represalias;
- existe un temor fundado de que la comunicación interna no se tramite correctamente;
- la infracción constituye un peligro inminente o manifiesto para el interés público.

2.2.2.2 Información útil sobre otros canales externos

También existen otros canales externos de comunicación de denuncias que pueden utilizarse:

- Entidad de Certificación DNV (feedback.Italia@dnv.com) y/o SAAS - Social Accountability Accreditation Services (saas@saasaccreditation.org), en el ámbito del sistema de certificación SA8000 y con el fin de verificar el mantenimiento de los requisitos correspondientes.
- Entidad de Certificación Bureau Veritas u otra entidad certificadora que esté vigente dentro del Grupo.
- Inspección Nacional de Trabajo (Ispettorato Nazionale del Lavoro), de forma directa o a través de la organización sindical de referencia del trabajador.

2.2.3 Revelación pública

La revelación pública consiste en hacer pública información sobre infracciones a través de la prensa, medios electrónicos u otros medios de difusión capaces de llegar a un gran número de personas.
La revelación pública constituye una herramienta residual y solo puede beneficiarse de las garantías previstas para el informante en los casos expresamente previstos por la ley, generalmente cuando no haya sido posible obtener un seguimiento adecuado a través de los canales de comunicación internos o externos o cuando exista un peligro inminente para el interés público.
Para el detalle de los requisitos y condiciones de uso de la revelación pública, se remite a las disposiciones normativas vigentes.

2.2.4 Denuncia ante la Autoridad

El D.Lgs. 24/2023 en materia de whistleblowing reconoce a los informantes la posibilidad de dirigirse directamente a la Autoridad Judicial o al Tribunal de Cuentas competente cuando tengan conocimiento de hechos que puedan constituir un ilícito o que sean relevantes desde el punto de vista penal, civil, administrativo o contable.
La presentación de una denuncia ante la Autoridad Judicial o el Tribunal de Cuentas constituye un canal autónomo respecto de los canales de comunicación internos y externos y puede beneficiarse de las medidas de protección previstas por la normativa aplicable, en las condiciones y con los límites que esta establece.
El Grupo garantiza el respeto de los derechos y garantías reconocidos por la ley a las personas que, actuando de buena fe y con motivos razonables, opten por presentar una denuncia ante las Autoridades competentes.
Para las modalidades, requisitos y condiciones de acceso a las garantías previstas en caso de denuncia ante la Autoridad Judicial o el Tribunal de Cuentas, se remite a la normativa vigente.
Para las Entidades en España, las informaciones podrán dirigirse asimismo al Ministerio Fiscal, a la Fiscalía Europea cuando afecten a los intereses financieros de la Unión Europea, y a los órganos jurisdiccionales competentes, de conformidad con la legislación procesal aplicable.

2.2.5 Comunicaciones realizadas de mala fe

El sistema de comunicación debe utilizarse de forma responsable, correcta y conforme a los principios de buena fe y lealtad.

Se consideran realizadas de mala fe las comunicaciones que resulten deliberadamente falsas, manifiestamente infundadas o presentadas con la intención de causar daño, perjuicio o desventaja a personas, sociedades u otras partes interesadas, así como las realizadas mediante el uso consciente de información falsa o gravemente distorsionada.
La protección prevista por la normativa de Whistleblowing no se extiende a quienes realicen comunicaciones con dolo o culpa grave, sin perjuicio de la protección reconocida a quienes hayan realizado una comunicación de buena fe sobre la base de elementos que consideraban razonablemente fiables en el momento de la comunicación, aun cuando las comprobaciones posteriores excluyan su fundamento.
La constatación de la mala fe podrá dar lugar a la adopción de las medidas disciplinarias, contractuales o de otra índole previstas por la normativa vigente y por las disposiciones de la empresa aplicables, sin perjuicio del derecho de la sociedad y de las personas interesadas a actuar ante las instancias competentes para la defensa de sus derechos e intereses.
La mera falta de fundamento de la comunicación, cuando el informante haya actuado de buena fe y con motivos razonables, no constituye por sí sola un elemento suficiente para considerar que la comunicación se ha realizado de mala fe.
Para las Entidades en España, comunicar o revelar públicamente información a sabiendas de su falsedad constituye una infracción muy grave conforme al artículo 63 de la Ley 2/2023, sancionable por la autoridad competente. Asimismo, quedan excluidas de la protección legal, entre otras, las personas que comuniquen informaciones inadmitidas por algún canal interno o por alguna de las causas previstas en el artículo 18.2.a) de la Ley 2/2023 (art. 35).

2.3 El Gestor de las Comunicaciones

El Gestor de las Comunicaciones puede ser una persona interna de la organización, un departamento, un comité o una persona externa. Cada sociedad del Grupo designa su propio Gestor de las Comunicaciones.
En caso de ausencia del Gestor de las Comunicaciones, este será sustituido por el Departamento de Risk&Compliance del Grupo.
Cuando la comunicación se refiera al Gestor de las Comunicaciones o implique un potencial conflicto de interés, deberá transferirse a una persona alternativa previamente designada por la sociedad afectada.
Para las Entidades en España, el órgano de administración designa y cesa al Responsable del Sistema, que actuará con independencia y autonomía, sin recibir instrucciones y con los medios necesarios. Su nombramiento y cese se notificarán a la A.A.I. o a la autoridad autonómica competente en el plazo de diez días hábiles (art. 8 de la Ley 2/2023).
La gestión del canal interno podrá externalizarse, sin que ello traslade la responsabilidad sobre el Sistema, que seguirá correspondiendo al Responsable del Sistema (art. 6).

2.4 Proceso de gestión de las comunicaciones internas

La comunicación puede realizarse por escrito (directamente a través del portal de whistleblowing, por correo electrónico o por correo postal ordinario) y de forma verbal (mensaje de voz o reunión presencial).

2.4.1 Recepción

Las comunicaciones recibidas a través de los canales internos son registradas y asumidas por el Gestor de las Comunicaciones designado por la sociedad afectada. El Gestor de las Comunicaciones está obligado a informar al informante, en un plazo de 7 días, de la recepción de la comunicación.

Se precisa que el acuse de recibo no implica, para el gestor, ninguna valoración del contenido de la comunicación, sino que tiene un carácter meramente informativo frente a la persona informante.

2.4.2 Evaluación preliminar e instrucción

El Gestor de las Comunicaciones somete la comunicación a una verificación preliminar con el fin de:

- evaluar su admisibilidad;
- verificar su pertinencia respecto del ámbito de aplicación;
- identificar la función competente para su gestión.

Cuando sea necesario, podrán solicitarse aclaraciones o información complementaria.

Una vez completada la actividad de comprobación, el Gestor de las Comunicaciones podrá:

- archivar la comunicación por infundada, motivando las razones;
- dirigirse a las funciones competentes para el correspondiente seguimiento.

Una vez identificada la función competente, que también puede ser el propio Gestor de las Comunicaciones, la comunicación se remite a efectos del inicio de la instrucción.

El Gestor de las Comunicaciones debe dejar constancia de cada comunicación en un registro **MD.PO.SGI.10-01** en el que se asignará a la comunicación un número correlativo "nombresociedad_#", donde "#" representa un número correlativo ascendente. En el registro se anotará, además, cuando proceda:

- la función competente y su contacto de referencia;
- el tema/asunto;
- si la instrucción está abierta o cerrada;
- si se prevén acciones consiguientes.

El registro deberá identificarse mediante un ID añadido al nombre del archivo con la fecha de la última actualización, p. ej., "MD.PO.SGI.10-01_Reporting Register_ddmmaaaa".

El Gestor de las Comunicaciones está obligado a dar respuesta a la persona informante en un plazo de 3 meses sobre el resultado de su comunicación:

- archivo;
- constatación de su fundamento y traslado a los órganos competentes.

Cuando la instrucción se cierre, deberá comunicarse al Gestor de las Comunicaciones, que procederá a actualizar el registro.

Para las Entidades en España, el plazo máximo para dar respuesta a las actuaciones de investigación no podrá ser superior a tres meses a contar desde la recepción de la comunicación o, si no se remitió acuse de recibo al informante, desde el vencimiento del plazo de siete días después de efectuarse la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso este podrá extenderse hasta un máximo de otros tres meses adicionales (art. 9.2.d) de la Ley 2/2023). Durante la tramitación podrá mantenerse la comunicación con el informante y, si se considera necesario, solicitarle información adicional.

La persona afectada tendrá derecho a que se le informe de las acciones u omisiones que se le atribuyen y a ser oída en cualquier momento, en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación. Se respetarán en todo caso la presunción de inocencia, el derecho de defensa, el derecho de acceso al expediente en los términos legalmente previstos, el honor de las personas afectadas y la confidencialidad de su identidad y de los hechos (arts. 9.2.f) y 39 de la Ley 2/2023).

Cuando los hechos pudieran ser indiciariamente constitutivos de delito, el Responsable del Sistema remitirá la información al Ministerio Fiscal con carácter inmediato o, en el caso de que los hechos afecten a los intereses financieros de la Unión Europea, a la Fiscalía Europea (art. 9.2.j) de la Ley 2/2023).

2.4.3 Definición de las acciones consiguientes

Al término de las verificaciones se determinan las eventuales acciones correctivas, preventivas o disciplinarias que se consideren necesarias, conforme a las disposiciones internas aplicables.
También en este caso será necesario informar al Gestor de las Comunicaciones de si se prevén o no acciones. No será necesario facilitar detalles, sino simplemente indicar si están previstas o no. Los detalles, en su caso, deberán ser facilitados por la función competente si se solicitan.

2.4 Reporting y seguimiento

Cada trimestre, el Gestor de las Comunicaciones envía a la función de Risk&Compliance del Grupo, a la dirección sgi@polygon.eu , un correo electrónico con el registro adjunto. Este flujo garantiza un seguimiento periódico con el fin de:

- identificar áreas de mejora;
- evaluar la eficacia de los controles internos;
- identificar posibles tendencias o incidencias recurrentes;
- apoyar la mejora continua de los procesos de la empresa.

Los resultados de las actividades de seguimiento podrán compartirse con los órganos y funciones competentes según sus respectivas responsabilidades.

2.5 Conservación de la documentación

La documentación relativa a las comunicaciones se conserva conforme a los plazos y modalidades previstos por la normativa aplicable, por los procedimientos internos y por las reglas de conservación documental adoptadas por cada sociedad del Grupo.
Para las comunicaciones de whistleblowing, el plazo de conservación no excede de 5 años.
Para las Entidades en España, el registro MD.PO.SGI.10-01 tendrá la consideración de libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar, conforme al artículo 26 de la Ley 2/2023. Este registro no será público y únicamente a petición razonada de la autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo su tutela, podrá accederse total o parcialmente a su contenido. Los datos personales relativos a las informaciones recibidas y a las investigaciones internas solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con la Ley 2/2023 y, en ningún caso, por un período superior a diez años.

2.6 Régimen de whistleblowing y Modelo 231

El Whistleblowing forma parte integrante del sistema de control interno y de compliance del Grupo y constituye una herramienta de apoyo a la aplicación eficaz del Modelo de Organización, Gestión y Control que, en su caso, se haya adoptado conforme al D.Lgs. 231/2001.
Las comunicaciones que pongan de manifiesto hechos, comportamientos o circunstancias potencialmente relevantes a efectos del D.Lgs. 231/2001 se gestionan en coordinación con las personas y órganos competentes designados por la sociedad afectada.

- Cuando el Organismo de Vigilancia haya sido designado como Gestor de las Comunicaciones, actuará conforme a las modalidades previstas en el presente procedimiento, asegurando la gestión de las comunicaciones y el desarrollo de las actividades de evaluación y análisis de su competencia.
- Cuando el Gestor de las Comunicaciones sea distinto del Organismo de Vigilancia, el Gestor asegurará la implicación tempestiva del Organismo de Vigilancia en las comunicaciones que presenten aspectos de potencial relevancia conforme al D.Lgs. 231/2001, respetando los

principios de confidencialidad, independencia, necesidad y minimización de la información compartida.

El Organismo de Vigilancia recibe la información necesaria para el desarrollo de sus actividades de supervisión del funcionamiento y cumplimiento del Modelo 231 y podrá formular recomendaciones o solicitar análisis adicionales en relación con los aspectos de su competencia.

La información derivada de las comunicaciones puede contribuir a las actividades de seguimiento de los riesgos, a la verificación de la eficacia del Modelo 231 y a la identificación de eventuales acciones correctivas o de mejora del sistema de control interno.

Para más detalles, se remite a los Modelos adoptados por cada sociedad del Grupo.

Para las Entidades en España, las referencias al Modelo 231 y al Organismo de Vigilancia se entenderán realizadas, respectivamente, al modelo de organización y gestión para la prevención de delitos previsto en el artículo 31 bis del Código Penal, cuando se haya adoptado, y al órgano de cumplimiento normativo (Compliance Officer u órgano equivalente) al que se haya confiado la supervisión de su funcionamiento y cumplimiento. El Sistema interno de información constituye, a estos efectos, el cauce para cumplir la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención (art. 31 bis.5.4.º del Código Penal).

2.7 Canal de comunicación compartido

En el ámbito del Grupo, una o varias sociedades podrán servirse de un canal de comunicación compartido, sin perjuicio del cumplimiento de los requisitos de confidencialidad, independencia, autonomía y protección de datos personales previstos por la normativa aplicable.

La adopción de un canal compartido tiene como finalidad favorecer la uniformidad de los procesos, la eficiencia en la gestión y la aplicación de estándares homogéneos en la recepción y gestión de las comunicaciones dentro del Grupo.

El uso compartido del canal no modifica la responsabilidad de cada sociedad respecto de la gestión de las comunicaciones de su competencia. Cada sociedad mantiene la responsabilidad de las evaluaciones, verificaciones y eventuales acciones consiguientes relativas a las actividades desarrolladas en su propio ámbito organizativo, salvo acuerdos distintos formalmente definidos.

Cuando el canal sea gestionado por una función centralizada o por una persona común a varias sociedades del Grupo, esta actuará con criterios de independencia, imparcialidad y ausencia de conflictos de interés, asegurando la correcta asignación de las comunicaciones a las personas competentes y la separación de la información cuando sea necesario.

Las modalidades organizativas y las responsabilidades relacionadas con el uso de canales compartidos son definidas por las sociedades afectadas conforme a la normativa aplicable y a los principios establecidos en el presente Procedimiento.

Para las Entidades en España, en el caso de un grupo de empresas conforme al artículo 42 del Código de Comercio, la sociedad dominante aprobará una política general relativa al Sistema interno de información y a la defensa del informante, y asegurará la aplicación de sus principios en todas las entidades que lo integran, sin perjuicio de la autonomía e independencia de cada sociedad, subgrupo o conjunto de sociedades integrantes que, en su caso, pueda establecer su respectivo sistema. El Responsable del Sistema podrá ser uno para todo el grupo, o bien uno para cada sociedad integrante de este, subgrupo o conjunto de sociedades, en los términos establecidos en dicha política (art. 11 de la Ley 2/2023). Asimismo, las Entidades en España que tengan entre cincuenta y doscientos cuarenta y nueve trabajadores podrán compartir entre sí el Sistema interno de información y los recursos destinados a la gestión y tramitación de las comunicaciones (art. 12 de la Ley 2/2023).

2.8 Protección de datos personales

Los datos personales obtenidos en el marco del proceso de comunicación se tratan conforme al Reglamento (UE) 2016/679 ("RGPD"), a la normativa nacional aplicable y a las disposiciones de la empresa en materia de protección de datos personales.

La información se trata exclusivamente para los fines relacionados con la recepción, gestión y verificación de las comunicaciones, conforme a los principios de minimización de datos y limitación del plazo de conservación.

Las sociedades del Grupo adoptan medidas técnicas y organizativas adecuadas para garantizar la seguridad, la confidencialidad y la integridad de la información tratada.

La información relativa al tratamiento de datos personales se facilita a los interesados mediante la correspondiente cláusula informativa de privacidad.

Para las Entidades en España, el tratamiento de datos personales se regirá, además, por la LOPDGDD y por el título VI de la Ley 2/2023. En particular:

- el acceso a los datos personales contenidos en el Sistema interno de información quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente a las personas previstas en el artículo 32.1 de la Ley 2/2023;
- no se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una información específica o, si se recopilan por accidente, se eliminarán sin dilación indebida;
- si se acreditara que la información facilitada o parte de ella no es veraz, se procederá a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal; y
- transcurridos tres 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 las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada.

3. Documentación relacionada

A continuación, se indica la documentación relacionada, que forma parte integrante del presente procedimiento:

- MD.PO.SGI.10-01 “Reporting Register”
- PL.PO.SGI.10-01 “Whistleblowing Policy”