



PROCEDIMIENTO DE GESTIÓN
DEL SISTEMA INTERNO DE
INFORMACIÓN
(PRCOM-GSE 003)

PROPIEDADES DEL DOCUMENTO

Título documento:	Procedimiento de Gestión del Sistema Interno de Información (PRCOM-GSE 003)	Versión:	2
Propietario:	Responsable del Sistema Interno de Información		
Aprobado por:	Consejo de Administración	Fecha de aprobación:	28/10/2025

HISTORIAL DE REVISIONES

VERSIÓN	FECHA	OBSERVACIONES
1.0	29/05/2023	Versión inicial
2.0	28/10/2025	Adaptación cambio proveedor canal ético

ÍNDICE

1. OBJETO	1
2. ÁMBITO DE APLICACIÓN Y ALCANCE.....	2
1.1. Ámbito Personal:	2
1.2. Ámbito Material:	2
3. DEBER DE INFORMAR.....	2
4. RESPONSABLE DEL SISTEMA DE INFORMACION	2
5. DERECHOS DE LAS PERSONAS QUE INFORMEN	3
6. DERECHOS DE LAS PERSONAS AFECTADAS POR LAS COMUNICACIONES	5
7. PROCEDIMIENTO DE INVESTIGACION DE LAS COMUNICACIONES RECIBIDAS EN EL SISTEMA DE INFORMACION	6
1.3. Fase de investigación	6
1.4. Fase de Conclusiones.....	10
8. COMUNICACIONES DE INFORMACIONES FALSAS O DE MAL FE.....	11
9. IMPOSICION DE MEDIDAS DISCIPLINARIAS.....	12
10. CANALES EXTERNOS Y AUTORIDAD INDEPENDIENTE	12
ANEXO I: COMITÉ DE COMPLIANCE (RESPONSABLE DEL SISTEMA)	13
ANEXO II: A.I.I COMPETENTES PARA LA COMUNICACIÓN DEL RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN Y CANALES EXTERNOS.....	14
ANEXO III: LISTADO ENUNCIATIVO DE REPRESALIAS PROHIBIDAS POR EL ARTICULO 36.3 DE LA LEY 2/2023	16

1. OBJETO

SIPCAM IBERIA, S.L., ("SIPCAM", la "Compañía" o la "Organización"), con ocasión de la implantación de un sistema de gestión de riesgos penales aprobó un Reglamento de Canal de Denuncias cuya finalidad era la comunicación por parte de los miembros de la Organización¹ de cualquier conducta contraria al Código Ético de la Compañía, así como cualquier sospecha de conducta ilícita o que pudiera generar un daño reputacional para Grupo SIPCAM.

Con la entrada en vigor de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción ("Ley 2/2023"), a los efectos de dar cumplimiento a lo dispuesto en el artículo 5.2. h) e i), se ha derogado el Reglamento existente y se ha procedido a la aprobación por parte del Consejo de Administración de SIPCAM de una Política del Sistema Interno de Información (la "Política") y del presente Procedimiento de gestión de las informaciones recibidas en el Sistema Interno de Información (el "Procedimiento").

A través del presente Procedimiento se regula la recepción, tratamiento, investigación y resolución de las comunicaciones que se reciban en el Sistema Interno de Información (el "Sistema") relacionadas con **conductas** de los miembros de la Organización que resulten **contrarias a la normativa interna de la Organización, a la legislación vigente**, cuando estas constituyan una **infracción administrativa grave, muy grave**, resulten **sospechosas de un ilícito penal** o cuando las anteriores pudieran constituir **infracciones del derecho de la Unión Europea** con relación sus **intereses financieros** o que incidan en **el mercado interior**.

El Sistema será fácilmente **accesible** a través de la **web corporativa** (<https://sipcamiberia.es/es/>) o directamente en el siguiente enlace: <https://canal-etico-broseta-compliance.i2-ethics.com/>. El presente Procedimiento garantiza la protección de los informantes, la posibilidad de trasladar informaciones anónimamente, la independencia y autonomía del Responsable del Sistema, la ausencia de conflictos de intereses en la gestión y en la realización de investigaciones internas, los derechos de defensa y presunción de inocencia y la celeridad en la gestión.

¹ Miembros de la Organización: integrantes del órgano de gobierno, directivos, empleados, trabajadores, empleados temporales o bajo convenio de colaboración, y voluntarios de una organización, y el resto de las personas bajo subordinación jerárquica de cualquiera de los anteriores.

2. ÁMBITO DE APLICACIÓN Y ALCANCE

1.1. Ámbito Personal:

Este Procedimiento resulta de aplicación a los miembros de la Organización, con carácter enunciativo, pero no limitativo, a los miembros del Consejo de Administración, directivos, personas que pudieran tener una relación profesional mercantil con la Organización, empleados, personal en prácticas y resto de partes interesadas.

1.2. Ámbito Material:

El Sistema debe entenderse como un instrumento de información que permita la comunicación de sospechas sobre las irregularidades e incumplimientos que se enuncian a continuación:

- Sospechas de actos, conductas, hechos u omisiones **contrarios a la legislación vigente**, cuando constituyan una **infracción administrativa grave, muy grave**.
- Sospechas de actos, conductas, hechos u omisiones que pudieran ser **constitutivas de un ilícito penal**.
- Sospechas de actos, conductas, hechos u omisiones que pudieran ser constitutivas de **infracciones del derecho de la Unión Europea** con relación sus **intereses financieros** o que incidan en **el mercado interior**.
- Sospechosas de actos, conductas, hechos u omisiones que pudieran ser constitutivas de **vulneración de la normativa interna de la Organización**.

3. DEBER DE INFORMAR

Los miembros de la Organización que tuvieran sospecha fundada de cualquier tipo de acto, hecho, conducta u omisión que pudiera resultar contrario a lo establecido en el apartado 2. del presente deberá ponerlo en conocimiento del Responsable del Sistema Interno de Información a través del Sistema puesto a disposición en la página web de SIPCAM.

4. RESPONSABLE DEL SISTEMA DE INFORMACION

El Consejo de Administración de SIPCAM, en virtud de lo dispuesto en el artículo 8.6. la Ley 2/2023 ha designado como Responsable del Sistema Interno de Información al **Comité de Compliance** de la Organización.

Se adjunta como **Anexo I** al presente procedimiento los datos de contacto de los **integrantes del Comité de Compliance**., así como la designación de la persona física encargada de la gestión y tramitación del Sistema Interno de Información conforme al artículo 8.2.

	PROCEDIMIENTO DE GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN	PRCOM-GSE 003 Rev 02 Sistemas de Gestión
---	--	---

5. DERECHOS DE LAS PERSONAS QUE INFORMEN

Los derechos que asisten al Informante desde la recepción de una comunicación en el Sistema de SIPCAM resultan los siguientes:

1. **Derecho a protección.** La Organización proporcionará protección a la persona que informen sobre las materias relacionadas en el apartado 2. del presente, denominado "*Ámbito material*", al objeto de evitar posibles represalias contra su persona. En el supuesto, de que el Informante hiciera público el contenido de la información, recurriendo a la denominada revelación pública, contemplada en el **artículo 27** de la Ley 2/2023 únicamente se podrá acoger a las medidas de protección cuando:
 - a. Hubiera denunciado primero a través del Sistema de SIPCAM.
 - b. Si existe riesgo manifiesto para el interés público. Entendiendo por tal una situación de emergencia o riesgo de daños irreversibles, incluido el daño para la integridad física
 - c. En caso de que se haya realizado una comunicación a través de un canal externo de información y existiera riesgo de represalias o pocas probabilidades de que se dé a la misma un tratamiento efectivo atendiendo a las circunstancias particulares del caso, por ejemplo, ocultación o destrucción de pruebas, connivencia con una autoridad, con el autor de la infracción o este se encuentre implicado en ella.
2. **Protección ante posibles represalias.** En ningún caso, SIPCAM, tomará represalia alguna contra el Informante, aun si del resultado de la investigación, se verificase que no ha existido un incumplimiento de la ley, siempre que no se haya obrado de mala fe. El autor de la represalia será sancionado. (El Anexo III del presente Procedimiento se recoge un listado enunciativo de represalias prohibidas por la Ley 2/2023).
3. **Derecho a recibir información.** El Informante será informado por escrito, una vez analizada la comunicación, sobre si esta es admitida a trámite o no. Una vez, haya finalizado la investigación, para el supuesto de la admisión de la comunicación, se dará traslado al Informante de las medidas de seguimiento previstas, así como del resultado de las investigaciones.
4. **Derecho a elegir.** El Informante, podrá elegir el cauce que considere más adecuado para remitir la información, pudiendo acudir a canales externos.
5. **De la información solicitada.** Podrá solicitarse al Informante, cuanta información se considere necesaria para la adecuada tramitación de la información, no pudiendo conservar el

Responsable del Sistema dicha información por un periodo superior a **diez (10) años**, tal y como establece el artículo 26.2 de la Ley 2/2023. La información facilitada no podrá ser utilizada para fines distintos a la investigación, cuestión que no resultará de aplicación en el supuesto de que se pudieran recibir comunicaciones relacionadas con los mismos hechos. Si los datos son transmitidos a una tercera persona para que investigue una comunicación, bien sea interna o externa, deberá informarse de tal cuestión al Informante, sin resultar necesario su consentimiento cuando la cesión de los datos esté autorizada por la legislación vigente. Los datos personales tratados como consecuencia de la presentación de una comunicación a través del Sistema de SIPCAM serán tratados conforme a lo dispuesto en el Reglamento General de Protección de Datos Personales, Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales, así como del resto de la normativa relacionada en vigor.

6. Derecho al anonimato.

7. Derecho a la confidencialidad. La identidad del Informante será confidencial, no pudiendo revelarse sin su consentimiento expreso a ninguna persona distinta para la gestión de las informaciones y la realización de las investigaciones internas. Las excepciones serán las que establece el derecho de la Unión Europea y la normativa española en el contexto de las investigaciones que puedan realizar las autoridades o en el transcurso de los procesos judiciales. SIPCAM garantiza la confidencialidad de la comunicación cuando esta fuera remitida por otros medios distintos al Sistema, así como cuando se hiciera llegar a través de miembros de la Organización no designados como Responsables del Sistema, en cuyo caso se advertirá a estos últimos, de que el quebrantamiento de la confidencialidad puede ser tipificado como una infracción muy grave. Asimismo, todos los miembros de la Organización, a través de formación, conocerán que en estos supuestos deberán remitirla con carácter inmediato al Responsable del Sistema de la Organización.

8. Derecho a recibir respuesta. El Informante recibirá un acuse de recibo de la información recibida en el plazo de **siete (7) días naturales** desde la recepción de la misma por parte del Responsable del Sistema Interno de Información. Este acuse de recibo podrá no remitirse en el supuesto de que el Responsable considere que con ello puede poner en peligro la confidencialidad de una comunicación. Con relación al **plazo** para la realización de la **investigación**, este no podrá ser superior a **tres (3) meses** a contar desde la recepción de la comunicación o, en caso de que no se hubiera remitido acuse de recibo al Informante, **tres (3) meses** a partir del **vencimiento del plazo de siete (7) días** después de efectuarse la comunicación, salvo en **casos de especial complejidad**, en los que se podrá ampliar el plazo por **tres (3) meses adicionales**.

9. **Derecho a la supresión de los datos.** Los datos personales relativos a las informaciones recibidas y a las investigaciones internas solo se conservarán durante el periodo que sea necesario y proporcionado. Concretamente, según lo establecido en el artículo 32.3 y 4 serán los siguientes:
- a. Los datos objeto de tratamiento solo podrán conservarse en el Sistema durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación.
 - b. Si se acredita que la información facilitada o parte de ella no es veraz, debe procederse a la inmediata supresión, salvo que la falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el **tiempo** necesario durante el que se **tramita el procedimiento judicial**.
 - c. Transcurridos los **tres (3) meses** desde la recepción de la comunicación sin que se hayan iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad sea dejar evidencia del funcionamiento del Sistema. En este caso podrán constar de manera anonimizada.
 - d. En ningún caso podrán conservarse los datos por un periodo superior a **diez (10) años**.

6. DERECHOS DE LAS PERSONAS AFECTADAS POR LAS COMUNICACIONES

Los derechos que asisten a la persona afectada desde la recepción de una comunicación en el Sistema de SIPCAM resultan los siguientes:

1. **Derecho a protección en el transcurso de la investigación.** SIPCAM proporcionará al Afectado la completa garantía de sus derechos, no siendo aplicables medidas sancionadoras, o legales, hasta que no se compruebe la veracidad de los hechos comunicados, se recaben evidencias y se concluya que se ha producido una infracción administrativa grave, muy grave, un ilícito penal, una vulneración de la normativa interna de la Organización o una conducta contraria a los intereses financieros de la Unión Europea o el mercado interior.
2. **Derecho a recibir información.** El Afectado tiene derecho a que se le informe de los actos, conductas, hechos u omisiones que se le atribuyen, así como a ser oído en cualquier momento. Dicha comunicación se realizará en el tiempo y forma que considere adecuado el Responsable del Sistema a los efectos de garantizar el buen fin de la investigación. La comunicación de información podrá retrasarse al objeto de que no se produzca destrucción o alteración de evidencias.

3. **Derecho a la confidencialidad.** Se deberá garantizar al Afectado la confidencialidad de sus datos personales al objeto de evitar que su difusión pueda afectar a su honorabilidad. Cuando se comuniquen los actos, hechos, omisiones, conductas o sospechas al Afectado, la comunicación se realizará sin revelar la identidad del Informante, salvo que se hubiera recabado el consentimiento expreso de este para tal fin.
4. **Derecho a una investigación objetiva y transparente.** El Afectado tiene derecho a la realización de una investigación objetiva, transparente y eficaz

7. PROCEDIMIENTO DE INVESTIGACION DE LAS COMUNICACIONES RECIBIDAS EN EL SISTEMA DE INFORMACION.

Se distinguen dos fases:

1. **Fase de investigación:** comprende la recepción y la evaluación inicial de la comunicación, con la correspondiente admisión o inadmisión de esta. Alcanza la investigación de los hechos comunicados, así como la recopilación de evidencias.
2. **Fase de conclusiones:** comprende el análisis de las evidencias, pruebas aportadas y la redacción del informe de conclusiones por parte del Responsable del Sistema. El informe contendrá la valoración de si corresponde la aplicación de medidas sancionadoras por parte del Consejo de Administración.

1.3. Fase de investigación

1.3.1. Comunicación y recepción de la comunicación

El Informante para interponer una comunicación en el Sistema deberá acceder al mismo a través de la página web de SIPCAM. Si son varios informantes, cada uno de ellos deberá interponer una comunicación. Las comunicaciones deben ser siempre individuales. Para el supuesto, de que se reciban a través del Sistema comunicaciones relacionadas con los mismos hechos, estas podrán fusionarse para la realización de un solo procedimiento investigador.

Antes de acceder al Sistema, el Informante deberá aceptar la Política del Sistema Interno de Información de SIPCAM, así como la Política en materia de protección de datos. Aceptadas ambas Políticas, se abre los siguientes campos para que puedan ser adecuadamente cumplimentados:

- Para el supuesto de que la **comunicación no sea anónima**:
 - Elección del tipo de comunicación:

- Acoso laboral o sexual.
 - Incumplimiento de la ley.
 - Sospecha de ilícito penal.
 - Incumplimiento de la normativa interna.
- Identidad del Informante.
- Correo electrónico.
- Descripción de los hechos.
- Posibilidad de adjuntar documentación: Word, pdf, imágenes o videos.
- Posibilidad de manifestar conflicto de intereses con el Responsable Sistema.
- Para el supuesto de que la **comunicación** fuera **anónima**:
 - Elección del tipo de comunicación:
 - Acoso laboral o sexual.
 - Incumplimiento de la ley.
 - Sospecha de ilícito penal.
 - Incumplimiento de la normativa interna.
 - Opción de anonimato.
 - Asignación de un código para el adecuado seguimiento.
 - Posibilidad de adjuntar documentación: Word, pdf, imágenes o videos.
 - Grabador de voz con distorsionador.
- Posibilidad de manifestar conflicto de intereses designado como con alguno de los miembros del órgano colegiado Responsable del Sistema.

Es importante que el Informante aporte detalle de los actos, conductas, hechos u omisiones comunicados, al objeto de poder realizar un adecuado análisis preliminar de la comunicación por parte del Responsable del Sistema.

A petición del Informante, también podrá presentarse la comunicación mediante una reunión presencial dentro del plazo máximo **de siete (7) días**. En este caso, se advertirá al Informante de la necesidad de dejar constancia del contenido de dicha reunión. Al igual que con las entrevistas que se mantengan con el Afectado y otros testigos, en la citada reunión, el Informante podrá elegir entre:

- La grabación de la conversación en un formato seguro, duradero y accesible.
- Transcripción completa y exacta de la conversación.
- Finalizada la reunión se entregará el acta al Informante para que pueda comprobar, rectificar y aceptar mediante su Organización la indicada transcripción.

Analizada la documentación adjunta a la comunicación el Responsable del Sistema podrá:

- **Admitir a trámite la comunicación:** por suponer los actos, conductas, hechos u omisiones comunicados contrarios a la normativa interna de la Organización, a la legislación vigente, pudieran constituir una infracción administrativa grave o muy grave, una sospecha de ilícito penal o fueran contrarios a los intereses financieros de la Unión Europea o el mercado interior.
- **Inadmitir la comunicación:**
 - Cuando los actos, conductas o hechos **carezcan de toda verosimilitud**.
 - Cuando los actos, conductas o hechos comunicados **no sean contrarios** a la normativa interna de la Organización, a la legislación vigente, pudieran constituir una infracción administrativa grave o muy grave, una sospecha de ilícito penal, una vulneración de la normativa interna de SIPCAM o no fueran contrarios a los intereses financieros de la Unión Europea o del mercado interior.
 - Cuando los actos, conductas o hechos comunicados **carezcan manifiestamente de fundamento o existan indicios de haberse obtenido la información a través de la comisión de un delito**, en cuyo caso además de la inadmisión se remitirá al Ministerio Fiscal.
 - Cuando los actos, conductas o hechos **no contengan información nueva y significativa sobre infracciones en comparación con una comunicación anterior** respecto de la cual ya se hubiera realizado y concluido un procedimiento investigador.

1.3.2. Inicio del procedimiento de investigación

Admitida la comunicación, el Responsable del Sistema procederá a la configuración de un expediente sobre la comunicación en investigación. Dicho expediente se gestiona a través de la herramienta informática destinada al efecto, la cual garantiza que ningún miembro de la Organización pueda acceder a los datos en ella contenidos por encontrarse en un servidor ajeno a SIPCAM.

La herramienta utilizada por SIPCAM tampoco permite alterar los registros en ella contenidos, así como dispone de un libro registro privado de todas las comunicaciones recibidas y de las investigaciones internas.

1.3.3. Equipo investigador

El equipo investigador lo conforma el Responsable del Sistema y a su vez Compliance Officer de SIPCAM, quien podrá recurrir a terceros externos para la realización de la investigación y recabar evidencias. En los supuestos en los que así lo considere, el Compliance Officer, podrá recabar colaboración de otros miembros de SIPCAM para realizar la investigación, siempre con las debidas garantías de confidencialidad y conforme a los principios de actuación que resultan aplicables al Responsable del Sistema y Compliance Officer.

El Responsable del Sistema podrá dirigirse a otras áreas de la Organización para solicitar y reclamar pruebas y evidencias, así como podrá solicitar colaboración a externos para el adecuado desarrollo de la investigación aplicando las garantías y principios referidos en el párrafo anterior.

La herramienta informática permite identificar posibles conflictos de intereses al Informante con carácter previo a trasladar una comunicación, en cuyo caso, la propia herramienta vetará al miembro del Responsable del Sistema el acceso al procedimiento de investigación en el que se encuentre conflictuado. Si recibida la comunicación se identificara un conflicto de intereses, el miembro Responsable del Sistema que presente el conflicto referido será excluido de la investigación.

1.3.4. Acciones de la investigación

El Responsable del Sistema emprenderán, cuantas acciones estimen convenientes al objeto de profundizar en los actos, conductas y hechos comunicados, al objeto de recabar información adicional para tomar una correcta decisión, de forma objetiva, en base a las evidencias recabadas. Con carácter enunciativo, pero no limitativo las acciones de investigación pueden ser las siguientes:

- Requerir nuevas evidencias y/o pruebas al Informante para mejorar el proceso de investigación.
- De común acuerdo con el Informante podrán acordarse las medidas cautelares necesarias relacionadas con cambios de puesto de trabajo y teletrabajo entre otras.
- Concertar entrevistas con el Informante, testigos, otros profesionales y con el Afectado. De las mencionadas entrevistas se obtendrá la siguiente evidencia:

- Grabación de la entrevista o acta literal de la entrevista mantenida.
- Compromiso de confidencialidad respecto de los hechos de los que haya tenido conocimiento que deberá ser por la Organización, por el Informante, testigos, otros profesionales y del Afectado.
- Revisión de toda la información relativa a la relación profesional de los implicados con la Organización, siempre con respeto a lo dispuesto en la legislación en materia de protección de datos y privacidad de los implicados.
- Colaboración de terceros externos.
- Análisis forense por externo experto independiente.
- Otras acciones que se consideren necesarias para continuar con el proceso de con el proceso de investigación, respetando la normativa vigente en Protección de Datos.

La investigación consistirá, en todo momento, de un análisis objetivo de la documentación disponible, la obtención de evidencias, recolección de pruebas y el análisis de estas.

El proceso de investigación durará como **máximo tres (3) meses** desde el día en que el Responsable del Sistema recibiera la comunicación o, **en caso de que no se hubiera remitido acuse de recibo al Informante, tres (3) meses a partir del vencimiento del plazo de siete (7) días** después de efectuarse la comunicación, **salvo en casos de especial complejidad, en los que se podrá ampliar el plazo por tres (3) meses** adicionales.

1.4. Fase de Conclusiones

7.2.1. Resolución

Una vez recabadas las pruebas y analizadas las mismas por parte del Responsable del Sistema, se procederá al cierre de la Fase de Investigación y se inicia la Fase de Conclusiones, en la que se procederá a la toma de decisiones respecto de la comunicación investigada, **proponiendo** al Consejo de Administración, las medidas que se recomiendo adoptar. El Consejo de Administración podrá las siguientes medidas:

- **Comunicación no procedente:** en el supuesto en el que la investigación de los actos, conductas y hechos comunicados se manifieste la ausencia de incumplimiento. El Responsable del Sistema informará al Informante y al Afectado de dicha decisión, junto con los motivos que sustentan la decisión.
- **Comunicación procedente:** En el supuesto que se pruebe que los actos, conductas o hechos comunicados son ciertos, se deberán detallar las acciones que sustentan dicha conclusión. El régimen sancionador se aplicará de conformidad con el Convenio Colectivo aplicable, la

legislación laboral, así como las obligaciones civiles o mercantiles que se hayan contraído con el miembro de la Organización.

7.2.2. Informe de Conclusiones

El Responsable del Sistema elaborará un informe de conclusiones reflejando el resultado de toda la fase de investigación. El informe de conclusiones contendrá:

- Aspectos técnicos: número de expediente, instructores, fecha de recepción de la comunicación, finalidad, nivel de confidencialidad (quién tiene acceso al mismo), código de identificación y fecha de cierre de la investigación.
- Antecedentes del expediente: actos, conductas o hechos que produjeron la comunicación, así como las personas o departamentos objeto de la investigación.
- Objeto de la investigación y su finalidad.
- Actuaciones, hechos relevantes investigados y detectados, evidencias y pruebas analizadas.
- Conclusiones determinadas, en base al objetivo y alcance de la investigación.
- Propuestas de medidas sancionadoras que deberá adoptar el Consejo de Administración, de conformidad con el Convenio Colectivo aplicable, la legislación laboral y el resto de las obligaciones civiles y mercantiles que haya contraído el miembro de la Organización Afectado, sin perjuicio de las responsabilidades penales que pudieran derivarse de la comisión de delitos.

El Responsable del Sistema recogerá dichas conclusiones de manera clara y concisa. Además, si existiera alguna limitación en el transcurso de la investigación, debe quedar reflejado en el informe.

De los informes resultantes se informará al Consejo de Administración a través de la Memoria Anual de actividades.

8. COMUNICACIONES DE INFORMACIONES FALSAS O DE MAL FE

El Sistema de Información de SIPCAM debe emplearse de manera responsable y adecuada. La comunicación de actos, conductas o hechos falsos, con una actitud maliciosa y moralmente deshonesto, que supone una infracción de la buena fe que debe presidir las relaciones de trabajo dentro de la Organización, pudiendo derivar en medidas disciplinarias de conformidad con el Convenio Colectivo Vigente.

Si, tras el oportuno análisis, se pudiera concluir que los hechos denunciados son manifiestamente falsos y que la comunicación ha sido presentada con actitud maliciosa y mala fe:

	PROCEDIMIENTO DE GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN	PRCOM-GSE 003 Rev 02 Sistemas de Gestión
---	--	---

- Se archivará la comunicación, documentando los motivos que han llevado a archivar el expediente, finalizando la labor de investigación.
- Se trasladará dicha circunstancia al Departamento de Human Resources (HR) de la Compañía, para que, en coordinación con el Responsable del Sistema, propongan medidas disciplinarias de conformidad con el Convenio Colectivo Vigente.
- Se informará de forma escrita, la propuesta de sanción al Consejo de Administración, quien decidirá la acción disciplinaria a aplicar al Informante de mala fe.

9. IMPOSICION DE MEDIDAS DISCIPLINARIAS

Si en la resolución de la investigación se comprobara que los actos, hechos o conductas comunicados son ciertos y están vinculados a conductas irregulares, ilícitas, constitutivas de infracciones administrativas graves o muy graves, contrarias a la legislación vigente, a la normativa interna de la Organización, a los intereses financieros de la Unión Europea o al mercado interior, el Afectado podrá ser objeto de sanción de conformidad con el dispuesto en el Convenio Colectivo aplicable, la legislación laboral, así como el resto de obligaciones civiles y mercantiles que haya contraído el miembro de la Organización.

Si el resultado de la investigación arroja indicios de comisión de un ilícito penal deberán ponerse los hechos en conocimiento del Ministerio Fiscal. Si se tratase de otro tipo de incumplimiento SIPCAM podrá poner los hechos en conocimiento de las autoridades judiciales si así lo considera necesario.

10. CANALES EXTERNOS Y AUTORIDAD INDEPENDIENTE

Ya sea directamente o previa comunicación a través de los medios señalados en el presente procedimiento, se podrá informar ante la **Autoridad Independiente de Protección del Informante (A.I.I.)**, o ante las autoridades u órganos autonómicos correspondientes, de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación de la *Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción*.

En el **Anexo II** del presente Procedimiento se informa acerca de las distintas A.A.I.I. autonómicas y estatales competentes que cuentan con un **Canal Externo**.

	PROCEDIMIENTO DE GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN	PRCOM-GSE 003 Rev 02 Sistemas de Gestión
---	--	---

ANEXO I: COMITÉ DE COMPLIANCE (RESPONSABLE DEL SISTEMA)

El Consejo de Administración de SIPCAM, en virtud de lo dispuesto en el artículo 8.6. la Ley 2/2023 ha designado como Responsable del Sistema Interno de Información al *Compliance Officer* de la Organización, compuesto por los siguientes miembros:

- **Xose Lois Devesa Novo:** Country Manager.
- **Simone Manetti :** Director Financiero.
- **Marta Ribes Vidal:** Directora de RRHH.

Dicho órgano ha delegado en Marta Ribes Vidal las facultades de gestión del Sistema Interno de Información, así como la tramitación de expedientes de investigación.

En el mismo acto y de conformidad con lo previsto en la Ley 2/2023, se acuerda notificar el nombramiento de esta persona designada, así como el de todos los integrantes del Órgano colegiado, a la Autoridad Independiente de Protección del Informante (A.I.I.) en el plazo legalmente establecido.

ANEXO II: A.I.I COMPETENTES PARA LA COMUNICACIÓN DEL RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN Y CANALES EXTERNOS

SIPCAM ha comunicado el nombramiento del Órgano Responsable de SII, así como sus integrantes, a la Agencia Valenciana Antifraude (AVAF), al encontrarse el domicilio social de la matriz del Grupo en la Comunidad Valenciana.

La AVAF es competente para actuar en las comunicaciones de incumplimientos que se encuentran relacionadas con:

- Las actividades de personas físicas o jurídicas que sean concesionarias de servicios o receptoras de ayudas o subvenciones públicas, a los efectos de comprobar el destino y el uso de las ayudas o las subvenciones.
- Las actividades de contratistas y subcontratistas que ejecuten obras de las administraciones públicas y de las entidades del sector público instrumental de la Generalitat, o que tengan atribuida la gestión de servicios públicos o la ejecución de obras públicas por cualquier otro título, con relación a la gestión contable, económica y financiera del servicio o la obra, y con las otras obligaciones que se derivan del contrato o de la ley.

Los datos de la AVAF para comunicar cualquier incumplimiento relacionado con su ámbito de actuación son los siguientes: (<https://avsre.gva.es/es/sistema-interno-informacion>):

- Por teléfono: +34 962787450
- Por correo electrónico: comunicacion@antifraucv.es
- Por correo postal: Calle Navellos, 14, puerta 3, 46003 València (España)

A continuación, le informamos de las distintas Autoridades Autonómicas competentes que cuentan en la actualidad con un canal externo en el que podrán comunicar cualquier incumplimiento relacionado con su ámbito de actuación:

Canal Externo Comunidad Autónoma	Vía de Acceso al Canal	¿Quién puede comunicar?
Cataluña	https://gencat.bustiaetica.s eu-e.cat/#/	Cualquier persona física o entidad que tenga conocimiento de infracciones o conductas corruptas o fraudulentas, cuando el incumplimiento comunicado se circunscriba al ámbito territorial de Comunidad Autónoma de Cataluña.

Canal Externo Comunidad Autónoma	Vía de Acceso al Canal	¿Quién puede comunicar?
Comunidad Valenciana	https://avsre.gva.es/es/sistema-interno-informacion	Cualquier persona física o entidad que tenga conocimiento de infracciones o conductas corruptas o fraudulentas, cuando el incumplimiento comunicado se circunscriba al ámbito territorial de Comunidad Autónoma de Valencia.
Galicia	https://www.es.parlamento.degalicia.es/Portada/SistemaInternoInformacion	Cualquier persona física o entidad que tenga conocimiento de infracciones o conductas corruptas o fraudulentas, cuando el incumplimiento comunicado se circunscriba al ámbito territorial de Comunidad Autónoma de Galicia.

De igual manera, se facilita información de los **Canales Externos de Comunicación** existentes a nivel europeo:

Canal Externo de Comunicación	Vía de Acceso al Canal
Buzón de Denuncias de la Oficina Europea de Lucha Contra el Fraude	https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_es
Canal de Denuncias ante la Fiscalía Europea	https://www.eppo.europa.eu/es/form/eppo-report-a-crime

	PROCEDIMIENTO DE GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN	PRCOM-GSE 003 Rev 02 Sistemas de Gestión
---	--	---

ANEXO III: LISTADO ENUNCIATIVO DE REPRESALIAS PROHIBIDAS POR EL ARTICULO 36.3 DE LA LEY 2/2023

- a) Suspensión del contrato de trabajo, despido o extinción de la relación laboral o estatutaria, incluyendo la no renovación o la terminación anticipada de un contrato de trabajo temporal una vez superado el período de prueba, o terminación anticipada o anulación de contratos de bienes o servicios, imposición de cualquier medida disciplinaria, degradación o denegación de ascensos y cualquier otra modificación sustancial de las condiciones de trabajo y la no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido; salvo que estas medidas se llevaran a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral o reguladora del estatuto del empleado público correspondiente, por circunstancias, hechos o infracciones acreditadas, y ajenas a la presentación de la comunicación.
- b) Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.
- c) Evaluación o referencias negativas respecto al desempeño laboral o profesional.
- d) Inclusión en listas negras o difusión de información en un determinado ámbito sectorial, que dificulten o impidan el acceso al empleo o la contratación de obras o servicios.
- e) Denegación o anulación de una licencia o permiso.
- f) Denegación de formación.
- g) Discriminación, o trato desfavorable o injusto.