



PROTOCOLO DE FUNCIONAMIENTO DEL SISTEMA INTERNO DE INFORMACIÓN

CONTROL DE VERSIONES

Versión	Causa cambio	Responsable	Fecha del cambio	Fecha de aprobación
1.0	Creación documento - Aprobación	Comité de Dirección	30/10/2023	30/10/2023

PROTOCOLO DE FUNCIONAMIENTO DEL SISTEMA INTERNO DE INFORMACIÓN

El presente protocolo se enmarca en el contexto de las políticas internas aprobadas por Agroseguro, fundamentalmente las siguientes:

- El Plan de Prevención de Riesgos Penales;
- El Código Ético y de Conducta;
- El Código de Buen Gobierno;
- La Política de Obsequios y Regalos; y
- La Política de Protección de Datos.

Este protocolo está destinado a establecer los canales para comunicar informaciones relativas a posibles irregularidades que se puedan producir en la entidad y que violen las políticas vigentes, así como a gestionar los procesos de investigación interna derivados de las mismas, como parte esencial del sistema de cumplimiento de la entidad.

En este sentido, el actual marco legislativo, en el cual se incluye, entre otras, 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 adelante, la Ley 2/2023), obliga al establecimiento de procedimientos y órganos de control y de comunicación internos para prevenir la realización de infracciones en el ámbito de aplicación de la citada Ley.

1. ¿Qué es el Sistema Interno de Información (SII)?

Es el cauce preferente para informar sobre:

- Acciones u omisiones que puedan constituir una infracción penal o administrativa grave o muy grave.
- Acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea, siempre que entren dentro del ámbito de aplicación de los actos de la Unión Europea enumerados en el anexo de la Directiva UE (2019/1937)¹, afecten a los intereses financieros de la UE o incidan en el mercado interior en el sentido del artículo 2 de la Ley 2/2023.
- Acciones u omisiones que puedan constituir una infracción de las políticas internas de la entidad, como el Código Ético, el Código de Buen Gobierno, la Política de Protección de Datos, la Política de Obsequios y Regalos, etc.
- Cualquier otra acción u omisión que pueda causar a la entidad un perjuicio constatable de cualquier clase.

En este sentido, el SII se asocia, sustituye y comprende al anterior Canal Ético y de Denuncias que servía como cauce para tener conocimiento sobre las posibles infracciones a las que se refieren los puntos anteriores.

¹ Principalmente, en materia de contratación pública; servicios, productos y mercados financieros, y prevención de blanqueo de capitales; seguridad y conformidad de productos; seguridad del transporte; protección del medioambiente; protección frente a radiaciones y seguridad nuclear; seguridad de los alimentos y piensos, sanidad animal y bienestar de los animales; salud pública; protección de los consumidores; protección de la privacidad y de los datos personales, y seguridad de las redes y sistemas de información.

2. ¿Para qué sirve el SII?

Para permitir que se pueda informar de una forma sencilla y eficaz sobre cualquiera de las situaciones expuestas anteriormente, garantizándose que no se vaya a producir ningún tipo de represalia o circunstancia negativa para el informante.

3. ¿Cuál es el fin del presente protocolo?

El establecimiento de unas reglas sencillas pero eficaces que regulen el funcionamiento del SII para que cualquiera pueda cumplir con su obligación de informar sin temor a represalias, garantizándose su confidencialidad y anonimato, y estableciéndose los mecanismos adecuados para que se respeten los derechos de la persona denunciada, incluyéndose, en todo caso, los reconocidos en la normativa de protección de datos de carácter personal.

Los criterios y pautas de actuación contenidas en este protocolo son de aplicación, principalmente, al Consejo de Administración, así como al Comité del Servicio de Información y Riesgos Penales (CSIRP), como entidad designada por aquel para la gestión de las informaciones, de acuerdo con lo establecido en la *Política de Gestión de Informaciones*, aprobada por el Consejo de Administración en su sesión de 24 de octubre de 2023.

Asimismo, el protocolo se aplicará a aquellas personas que estén involucradas en la recepción, tramitación, investigación o adopción de medidas que puedan derivarse de la comunicación de información recibida tales como, por ejemplo, las personas que participen en la investigación de los hechos, cuya involucración se solicitará a criterio del Comité del Servicio de Información y Riesgos Penales (CSIRP).

4. ¿Quién puede usar el SII?

Podrán ser informantes todas aquellas personas que hayan obtenido información sobre alguna de las infracciones expuestas, pertenezcan o no a la empresa, como son:

- Todos los empleados de la entidad, incluidos becarios, trabajadores en formación, etc.
- Los administradores
- Los accionistas.
- Los terceros que tengan algún tipo de vínculo con la actividad de la entidad, ya sea mercantil, profesional o de otro tipo, como, por ejemplo, autónomos, contratistas, subcontratistas, proveedores, auditores, consultores, administraciones públicas, etc.

Dichas personas podrán ser tanto físicas como jurídicas, en este último caso a través de las personas físicas que trabajen para ellas.

La información que se comunique podrá ser sobre hechos conocidos durante su relación con la entidad, una vez finalizada esta o incluso si la misma aún no ha llegado a iniciarse o no se inicia, por haber sido obtenida, por ejemplo, durante un proceso de selección o de una negociación precontractual, etc.

5. ¿Qué puedo informar o comunicar a través del SII?

Que se haya producido, se esté produciendo o exista el riesgo de que se pueda producir alguna de las infracciones expuestas, así como que se estén incumpliendo o resulten objetivamente ineficaces los controles previstos para evitar la realización de dichos comportamientos.

6. ¿Tengo obligación de acudir al SII?

Todos los empleados de Agroseguro, sea cual sea su cargo, los miembros del órgano de administración, y aquellos que realicen las auditorías o desempeñen funciones propias de la empresa de forma externalizada, tienen la obligación de comunicar a través del SII la existencia de posibles infracciones o incumplimientos que pudieran dar lugar a ellas.

7. ¿Cuándo hay que acudir al SII?

En cuanto se tenga noticia de alguna de las infracciones o situaciones relacionadas en el apartado 1 o de la posible ineficacia o idoneidad de los controles previstos para su evitación. La comunicación se hará con la mayor celeridad posible, tan pronto como se conozca la potencial infracción.

8. ¿Cómo puedo contactar e informar de una posible infracción a través del SII?

Existen varias vías posibles:

- A través del formulario que figura en la página de inicio de la web de Agroseguro (www.agroseguro.es) en la pestaña: “Sistema Interno de Información (SII)” (vía recomendada).
- Por correo electrónico a la dirección: servicioinfo@agroseguro.es
- Verbalmente a través número de teléfono **919101591**. La conversación, una vez informado de ello el informante y recogido su consentimiento, será grabada en un formato seguro, duradero y accesible.
- Por mensajería de voz a través del anterior número telefónico.
- Presencialmente, ante el propio Comité, pidiendo cita previa a través del número telefónico o el correo electrónico citados anteriormente. En ambos casos, se fijará en ese momento la reunión, que tendrá que celebrarse dentro de los siguientes siete días hábiles, salvo imposibilidad justificada de las partes, en cuyo caso se celebrará lo antes posible.
- Por correo postal a la dirección:

AGROSEGURO
Comité del Servicio de Información y Riesgos Penales
C/ Gobelos 23
(28023 – Madrid)

En caso de formular denuncia por correo postal, se recomienda no poner remitente, para preservar la confidencialidad y anonimato de la misma.

- Es posible facilitar la información o comunicación de forma anónima sin facilitar la identidad del informante. En este caso, no será posible informarle del estado del expediente, ni solicitar la subsanación de la falta de alguno de los requisitos necesarios para su tramitación, por lo que, de resultar inviable la investigación de los hechos que figuran en la información o comunicación, esta no podría subsanarse y sería inmediatamente eliminada.

En la informaciones o comunicaciones recibidas de forma confidencial, se enviará al informante acuse de recibo de la comunicación realizada dentro del plazo de siete días.

A los informantes se les informará igualmente de los canales externos de información ante aquellas autoridades nacionales o europeas que pudieran resultar competentes.

9. ¿Quién va a saber que soy el informante?

Solo los miembros del Comité del Servicio de Información y Riesgos Penales (CSIRP), órgano responsable del SII, van a conocer su identidad. Los miembros del CSIRP son: el jefe del departamento de Recursos Humanos, el responsable de Control Interno y el jefe del departamento de Asesoría Jurídica.

Estos están sujetos a la obligación de confidencialidad, y no facilitarán la identidad del informante a la persona involucrada ni a ningún otro empleado de la empresa o persona relacionada de alguna forma con los hechos o las personas implicadas, salvo que, por la naturaleza del hecho, resultase absolutamente necesario comunicárselo a los empleados que tuvieran que intervenir directamente en la investigación, quienes tendrán, en todo caso, que firmar una hoja de confidencialidad de información que recibirán a tal efecto.

La identidad del informante se podrá comunicar a los profesionales externos (abogados, auditores, peritos, etc.) que participen en la investigación, quienes también estarán sometidos al mismo deber y régimen estricto de confidencialidad.

Asimismo, la identidad del informante se comunicará al juez, fiscal, policía o autoridad administrativa a quien se traslade el resultado de la investigación en caso de resultar la misma jurídicamente relevante desde el punto de vista penal o administrativo.

Lo anterior no podrá ser, obviamente, de aplicación en caso de facilitar la información o comunicación de forma anónima.

La Organización ha implementado procedimientos que garantizan la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, de las actuaciones que se desarrollen en su gestión y tramitación, así como la protección de datos, impidiendo el acceso de personal no autorizado.

10. ¿Qué sucede si la persona a la que se refiere la información es un miembro del propio CSIRP?

En este caso, la información o comunicación se realizará de la misma forma, con la diferencia de que la persona afectada no podrá participar en forma alguna en la tramitación y resolución del expediente.

En el supuesto de que el informante considere necesaria la práctica previa de pruebas o que el conocimiento *ab initio* del informante del CSIRP pudiera comprometer su práctica o comprometer la calidad de la existente, y con el fin de salvaguardar dichas pruebas, el informante, de forma excepcional, podrá iniciar el trámite a través del correo personal de alguno del resto de los miembros del CSIRP, cumpliendo en todo caso los requisitos establecidos con carácter general para su admisión. Una vez recibida la información o comunicación, si se ha formulado solo ante uno de los miembros, este lo pondrá en conocimiento del otro, manteniéndose, como en el resto de los casos, el deber de confidencialidad y tramitándose el expediente de igual forma y dando el mismo tratamiento al miembro afectado que se daría a cualquier otro.

11. ¿Qué contenido deben tener las informaciones o comunicaciones?

Tanto si se hace verbalmente como por escrito, deberá tener necesariamente el siguiente contenido:

- Identidad del informante (nombre y apellidos), salvo en supuestos de denuncias anónimas.
- Identidad de la persona o personas a las que se refiere la información o comunicación, si se conoce (nombre y apellidos).
- Descripción lo más detallada posible de los hechos.
- Indicios o pruebas sobre los que se basa la información. Se deberán aportar todos los elementos probatorios de que se disponga. En caso de no tenerlos en su poder, se identificará dónde y cómo se pueden obtener. Si hubiera que practicar prueba para acreditar los hechos que dependa de la empresa o de personas relacionadas con esta, la misma se solicitará también al CSIRP.

12. ¿Cómo se tramita la información o comunicación?

En el momento en que el CSIRP reciba la información o comunicación, procederá a evaluar su contenido, comprobando:

- Que contiene la información mínima prevista en el punto anterior.
- Que los hechos descritos pueden ser constitutivos de un hecho sujeto a su competencia.
- Que los hechos descritos tienen una mínima base de credibilidad y/o de prueba de que no se trata de una mera valoración subjetiva del informante, carente de indicio o base alguna de veracidad.
- Realizado lo anterior, acusará recibo escrito al denunciante (si la información no es anónima) en el plazo máximo de siete días naturales desde su recepción, dándole un código de identificación del expediente para facilitar su seguimiento y comunicándole expresamente la posibilidad de mantener comunicación con el informante y la posibilidad de solicitar información adicional si fuera necesario, ya sea en dicho momento o en un futuro, de acuerdo a cómo evolucione la instrucción del expediente.

En el caso de que falte alguno de los requisitos previstos en este punto, se requerirá al informante en el plazo de 10 días hábiles desde la recepción para que subsane la falta en un plazo de 5 días hábiles.

El CSIRP archivará el expediente mediante informe escrito y motivado si:

- No se cumpliera, en el plazo previsto, el requerimiento de subsanación, salvo causa justificada.
- Los hechos informados carecieran de la más mínima base de veracidad, sin prueba o indicio alguno en base al cual pudiera, aun indiciariamente, presumirse la realidad de los hechos, o bien no se hubieran aportado, pese a haber sido solicitados, los extremos incluidos en el escrito de subsanación.

En estos casos, el expediente se eliminará sin quedar registro o constancia del mismo, con el fin de evitar un registro de “antecedentes” no probados que pudiera incidir en la presunción de inocencia y el derecho al honor de la persona afectada.

En caso de que se cumplan los requisitos de admisión a trámite de la denuncia, o una vez subsanadas las deficiencias, el CSIRP:

- Registrará la misma.
- Informará al informante, en el plazo de siete días hábiles, de la iniciación de la investigación y su número de expediente, de cuyo resultado asimismo se le informará en su momento por escrito y se le facilitará la información de sus derechos de acceso y rectificación, salvo en supuestos de denuncias anónimas.
- Iniciará y dirigirá la debida investigación interna para averiguar si los hechos comunicados son ciertos, practicando aquellas pruebas (documentales, testificales, periciales) que resulten necesarias y aquellas solicitadas por el propio informante que se estimasen posibles y pertinentes.
- El plazo de tramitación de la investigación será de 30 días hábiles desde la recepción o subsanación, salvo que deba practicarse prueba, para lo cual quedará suspendido el plazo desde que se pida hasta que se obtenga la misma, reflejándose por escrito tal circunstancia en el expediente y reanudándose el computo del plazo que reste desde que se disponga de la misma. En todo caso, la fase de investigación no podrá superar los 3 meses a contar desde la recepción de 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.
- Se dejará constancia documental de todas las pruebas practicadas, incluso las testificales. El CSIRP podrá tomar declaración a la persona afectada, si esta accede a ello.
- El informante deberá aportar al CSIRP aquellas pruebas de las que pueda tener conocimiento con posterioridad a iniciarse el procedimiento.
- El informante podrá pedir verbalmente o por escrito, en el momento de la denuncia o posteriormente, una reunión presencial con el CSIRP, la cual se celebrará dentro de los siete días naturales siguientes.
- El afectado será puntualmente informado de los hechos por los que se le va a investigar, teniendo en todo momento derecho a ser oído, pudiendo presentar alegaciones por escrito en cualquier momento y, en todo caso, cuando el CSIRP se lo pida, siempre antes de la resolución del expediente. En el caso de que la comunicación de la información recibida a la persona afectada pudiera entorpecer de algún modo la investigación interna, dicha comunicación podría demorarse por el tiempo estrictamente necesario para realizar aquellas diligencias probatorias concretas que pudieran verse entorpecidas, dejando informe escrito, previo y motivado, de tal decisión en el expediente. Todas las actuaciones se realizarán teniendo muy presente la presunción de inocencia y el derecho al honor de la persona afectada.
- Todas las actuaciones y decisiones, aún de mero trámite, se recogerán por escrito en el expediente, así como las pruebas facilitadas y el resultado de las que se practiquen.
- Las decisiones del CSIRP se tomarán por mayoría y de forma motivada. En caso de que no sea por unanimidad, el miembro del CSIRP en minoría emitirá el correspondiente voto particular motivando su decisión. Todas las decisiones formarán parte del expediente, que quedará archivado en el CSIRP.
- El CSIRP comunicará al informante por escrito la resolución del expediente, salvo en supuestos de denuncias anónimas.

- En caso de considerarse acreditados los hechos y ser los mismos relevantes, se elevará la resolución a la dirección de la empresa y se impondrán, tan pronto como sea posible, las sanciones disciplinarias correspondientes, entregándose, de ser el caso, el resultado de la investigación al juez, fiscal, policía o autoridad administrativa a quien corresponda para que pueda proceder en consecuencia.
- Si el informante o los propios miembros del CSIRP conocieran con posterioridad al archivo de un expediente nuevas pruebas que pudieran cambiar el sentido de la resolución tomada, deberán aportarlas, procediéndose, en tal caso, a reabrir el expediente informando al afectado de forma inmediata.
- Todas las actuaciones se realizarán respetando la normativa sobre protección de datos y demás normativa de aplicación.

13. ¿Qué derechos y obligaciones tiene el informante?

a) Derechos

Confidencialidad: solo el CSIRP conocerá su identidad. Si alguien más la tuviera que conocer por necesidad en la tramitación del expediente, deberá firmar previamente un acuerdo de confidencialidad en tal sentido. El ejercicio de los derechos de acceso y rectificación por parte del afectado no incluye la revelación de los datos identificativos del informante.

No represalias: se prohíbe de forma terminante a cualquier persona la adopción de cualquier sanción, represalia o consecuencia negativa contra una persona por el hecho de haber facilitado una información o haber realizado una comunicación.

El incumplimiento de las garantías de confidencialidad y no represalias previstas en los puntos anteriores constituye una infracción muy grave en el sistema disciplinario de Agroseguro. No obstante, estas garantías de confidencialidad y no represalias citadas anteriormente, no se aplicarán a informaciones o comunicaciones realizadas con conocimiento de su falsedad o con temerario desprecio hacia la verdad, que igualmente constituyen una infracción muy grave en el sistema disciplinario.

b) Obligaciones

Veracidad: el informante tiene que responder, en cualquier caso y en la medida de lo posible según el caso concreto, de la veracidad de los datos facilitados. El responsable de la tramitación se tiene que reservar el derecho a rechazar las informaciones que sean falsas, sin perjuicio de las demás acciones que procedan en Derecho.

14. Protección de datos personales.

a) ¿Quién es el responsable de tratar los datos personales?

Agrupación Española de Entidades Aseguradoras de los Seguros Agrarios Combinados, S.A. (Agroseguro). CIF: A28637304. Dirección postal: calle Gobelas, 23 (28023 – Madrid). Correo electrónico: agro@agroseguro.es. Contacto del Delegado de Protección de Datos: dpd@agroseguro.es

b) ¿Para qué utilizamos los datos?

Para tramitar las correspondientes informaciones o comunicaciones que se puedan realizar de conformidad con lo establecido en este protocolo.

En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones a las que se refiere el apartado 1. *¿Qué es el Sistema de Información Interno?*, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la ley.

Si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda a su registro y tratamiento.

c) ¿Cuánto tiempo almacenaremos sus datos?

Los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.

En todo caso, se procederá a su destrucción transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema. Las comunicaciones a las que no se haya dado curso solamente se almacenarán de forma anonimizada.

Igualmente, se procederá a su inmediata supresión si se acredita que la información facilitada o parte de ella no es veraz, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

En ningún caso los datos incluidos en el registro de informaciones se conservarán por un periodo superior a diez años.

d) ¿Cuál es la base legal para utilizar sus datos?

La justificación legal se fundamenta en:

- Misión realizada en interés público.
- Cumplimiento de obligaciones legales.

e) ¿A quién comunicaremos sus datos?

El acceso a los datos contenidos en estos sistemas queda limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, formen parte del CSIRP, al delegado de protección de datos de la organización o a los encargados del tratamiento que eventualmente se designen a tal efecto entre otros profesionales externos (abogados, auditores, peritos, etc.). No obstante, será lícito su acceso por otras personas cuando resulte necesario para la adopción de medidas correctoras en la entidad o para la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan. Sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador, dicho acceso se permitirá al personal con funciones de gestión y control de recursos humanos.

La identidad del denunciante podrá comunicarse al juez, fiscal, policía o autoridad administrativa a quien se traslade el resultado de la investigación, en caso de resultar la misma relevante.

f) ¿Qué derechos posee en relación con estos datos?

Puede ejercer los derechos de acceso, rectificación, supresión, portabilidad, oposición y limitación presentando una solicitud a:

Agroseguro, SA
Comité del Servicio de Información y Riesgos Penales
Calle Gobelos, 23
28023 – Madrid

o a la dirección de correo electrónico servicioinfo@agroseguro.es, aportando copia de su DNI o documento oficial que le acredite.

No obstante, no procederá el ejercicio de tales derechos en los siguientes supuestos:

- Cuando la persona denunciada ejercite su derecho de acceso o rectificación, no se le comunicarán los datos identificativos del denunciante.
- Cuando el ejercicio de estos derechos se efectúe respecto de una denuncia relacionada con la prevención del blanqueo de capitales y financiación del terrorismo, en cuyo caso se aplicará lo dispuesto en el artículo 32 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y financiación del terrorismo.

Igualmente, tiene derecho a presentar la correspondiente reclamación ante la Agencia Española de Protección de Datos a través del siguiente enlace: www.aepd.es

15. Revisión y aprobación del Protocolo.

El presente *Protocolo de funcionamiento del Sistema Interno de Información* ha sido aprobado por el Comité de Dirección de la Entidad con fecha 30 de octubre de 2023 y publicado por los instrumentos de comunicación interna de la Entidad.

Se revisará con periodicidad anual, actualizando su contenido cuando proceda o en el momento en que se produzcan cambios relevantes.

Anualmente se emitirá un informe sobre la actividad del SII, que, además de la descripción de la misma durante el ejercicio anterior, contendrá las mejoras introducidas o a introducir. Dicho informe incluirá el actual y preceptivo Informe de Gestión de Riesgos Penales.