Procedimiento del Sistema Interno de Información

CONTROL DE VERSIONES.

Versión	Fecha	Control
1	26/06/2023	Elaboración y aprobación del Procedimiento
2	30/10/2023	Aprobación actualización del procedimiento
3	29/04/2024	Aprobación actualización del procedimiento
4	28/05/2024	Aprobación actualización del procedimiento
5	30/09/2024	Aprobación actualización del procedimiento

Índice

1. ANTECEDENTES Y OBJETO DEL PRESENTE PROCEDIMIENTO

Como consecuencia de la entrada en vigor, de la Ley Orgánica 5/2010, de 22 de junio, que supuso la modificación del Código Penal, introduciendo, entre otros puntos, la posibilidad de declarar la responsabilidad penal de las personas jurídicas, Caja Rural Nuestra Madre del Sol, S.C.A.C., en adelante la Caja o la Entidad, procedió al establecimiento de medidas tendentes a incorporar las previsiones establecidas en dicha regulación.

En el año 2020 la Caja implementó un Sistema de Gestión de Cumplimiento Penal (en adelante SGCP), estableciendo un modelo de organización, prevención, gestión y control de riesgos penales en relación con el régimen de responsabilidad penal de las personas jurídicas.

Como parte del Sistema anteriormente referido, el Canal Ético (antes denominado canal de denuncias) se configuraba como un mecanismo más de los adoptados por la Entidad en esta materia, muy útil a la hora de facilitar la toma de conocimiento de todas aquellas conductas cometidas en el seno de la organización que pudiesen ser constitutivas de delito así como incumplimientos del Código de Conducta de la Entidad, incumplimientos de la normativa de Prevención del Blanqueo de Capitales y Financiación del Terrorismo e irregularidades de naturaleza financiera y contable, y respecto de las cuales se haga necesario llevar a cabo la oportuna investigación de las mismas y, en su caso, la adopción de las medidas correctivas pertinentes para eximir o atenuar la responsabilidad penal de la Entidad.

La Entidad dispone de otros procedimientos internos con finalidades propias como el de prevención de blanqueo de capitales o como el protocolo para situaciones de acoso laboral o sexual o por razón de sexo.

El panorama anteriormente expuesto se modifica sustancialmente con la aprobación y 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, que introduce la obligación de conformar un Sistema Interno de Información (en adelante SII), homogeneizando los diversos canales de comunicación y ampliando el ámbito subjetivo y material de éstos.

La finalidad de la norma es la de proteger a las personas que en un contexto laboral o profesional detecten infracciones penales o administrativas graves o muy graves y las comuniquen mediante los mecanismos regulados en la misma. Por todo lo anterior, el Consejo Rector de la Caja, previa comunicación a los trabajadores con fecha 20 de junio de 2023, ha acordado aprobar una nueva Política de obligado cumplimiento que integre la Ley 2/2023 en el acervo normativo interno de la Entidad, estableciendo a través de la misma los fundamentos de nuestro Sistema Interno de Información, así como los principios y órganos internos responsables de asegurar su eficaz implantación.

Como desarrollo de la indicada Política, se establece este Procedimiento con el fin de poner a disposición de todos los integrantes de la Caja los medios necesarios para garantizar su cumplimiento efectivo en todo momento y circunstancia.

Así, este Procedimiento:

- Delimita el alcance de los diferentes canales de comunicación establecidos en la Entidad.
- Proporciona las pautas de actuación en caso de presentación de una denuncia, comunicación o consulta, estableciendo una guía adecuada para la gestión de aquellas en lo referente a su análisis, investigación interna y resolución.
- Identifica las funciones, roles y responsabilidades de cada una de las partes intervinientes en el proceso de actuación.

- Define las principales actuaciones a llevar por los gestores del SII de cara a entender y delimitar la naturaleza de las denuncias, comunicaciones y consultas recibidas, así como el análisis y reporte de los datos recabados.

Igualmente, el SII y los canales internos de información, que se habiliten en el marco de su desarrollo se configuran como un medio para que cualquier usuario del mismo, pueda dirigir consultas a los órganos habilitados para ello, relacionadas con cualquiera de los asuntos que entran dentro del ámbito de sus competencias, y obtener de estos el debido asesoramiento al respecto.

El Procedimiento contempla los principios y garantías consagrados en la Política del SII de la Entidad.

2. ALCANCE DEL SISTEMA INTERNO DE INFORMACIÓN

El alcance material del Sistema Interno de Información viene establecido en la Política del Sistema Interno de Información, donde se establece que podrá comunicarse conforme a lo establecido en el artículo 2 de la Ley 2/2023:

a) Cualquier acción u omisión que pueda constituir una infracción del Derecho de la Unión Europea siempre que

   a. entren dentro del ámbito de aplicación de los actos de la Unión Europea enumerados en el anexo de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno;

   b. afecten a los intereses financieros de la Unión Europea tal y como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE);

   c. o incidan en el mercado interior, tal y como se contempla en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión Europea en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades o con prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades

b) Cualquier acción u omisión que pueda ser constitutiva de infracción penal, o administrativa grave o muy grave entendiéndose en todo caso comprendidas las que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social y de forma particular, la infracción de la normativa reguladora de la prevención del blanqueo de capitales y financiación del terrorismo.

c) Especialmente cualquier conducta tipificada en el Código Penal que pudieran dar lugar a la responsabilidad penal de las personas jurídicas recogidas en el SGCP de la Entidad.

d) Cualquier irregularidad (error material o fraude) cometida en el proceso de emisión de Información Financiera y contable de la Entidad.

e) Cualquier infracción del Sistema de Gobierno Interno de la Entidad.

f) Las violaciones del Código de Conducta de la Entidad.

g) Cualquier conducta que pueda ser constitutiva de acoso laboral, sexual o por razón de sexo que pueda dar lugar al incumplimiento del Protocolo para la prevención del acoso sexual y acoso por razón de sexo.

En adelante, el conjunto de disposiciones legales y directrices internas mencionadas cuya infracción es susceptible de ser denunciada a través del SII y sus canales de comunicación, serán denominadas como "la Normativa".

Las comunicaciones deberán hacer referencia a acciones u omisiones que la Entidad tenga capacidad para investigar, corregir y reparar, es decir, relacionadas con las conductas de los miembros de la Entidad o del resto de partes interesadas o socios de negocio que participan de las actividades, procesos y procedimientos de la Entidad.

En cuanto al alcance personal, el SII ampara a todas las personas que informen sobre cualquier acción u omisión comprendida en el alcance material establecido en el apartado anterior, estableciendo un régimen de especial protección para las personas informantes contempladas en el artículo 3 de la Ley 2/2023 que se desarrolla en este procedimiento, dentro del ámbito material de aplicación del artículo 2 de dicha norma.

3. SISTEMA INTERNO DE INFORMACIÓN

La entidad Caja Rural Nuestra Madre del Sol, S.C.A.C. es la responsable del tratamiento de los datos del sistema interno de información. El Consejo Rector será quién tome las decisiones en nombre del responsable del tratamiento, y será responsable de su implantación, teniendo que designar para ello un responsable del sistema interno de información (persona física u órgano colegiado - si es órgano colegiado, este deberá delegar en uno de sus miembros las facultades de gestión del Sistema interno de información y de tramitación de expedientes de investigación-), según se indica en el apartado 5.

Por todo ello, en base al artículo 4 de la Ley 2/2023, el Sistema interno de información debe ser el cauce preferente para informar sobre las acciones u omisiones previstas en el artículo 2, siempre que se pueda tratar de manera efectiva la infracción y si el denunciante considera que no hay riesgo de represalia".

3.1. Requisitos del Sistema Interno de Información

El SII debe:

a) Permitir a las personas informantes y otros usuarios del SII comunicar información sobre las infracciones previstas en el artículo 2 de este procedimiento, de acuerdo con los principios establecidos en la Política del Sistema Interno de Información.

b) Estar diseñado, establecido y gestionado de una forma segura, de modo que se garantice la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, y de las actuaciones que se desarrollen en la gestión y tramitación de esta, así como la protección de datos, impidiendo el acceso de personal no autorizado.

c) Facilitar la presentación de comunicaciones por escrito o verbalmente, o de ambos modos y en su caso de forma anónima, en los canales cuya normativa lo permita.

d) Integrar los distintos canales internos de información que pudieran establecerse dentro de la Entidad, respetando la normativa específica que regule los diferentes canales.

e) Garantizar que las comunicaciones presentadas serán tratadas de manera efectiva, con el objetivo de investigar, corregir y reparar la posible irregularidad de la forma más inmediata.

f) Ser independiente el SII de cualquier otra organización y aparecer siempre diferenciado respecto al de otras entidades u organismos.

g) Contar con un Responsable del SII designado por el Consejo Rector, que mantendrá el rol, funciones y responsabilidades recogidas en el artículo 5 de este procedimiento.

h) Contar con un procedimiento de gestión de las informaciones recibidas en los términos establecidos en el apartado 8 de este procedimiento.

i) Establecer las garantías para la protección de los informantes y otros usuarios del SII y contar con procedimientos de protección a los informantes en los términos establecidos en el apartado 9 de este procedimiento.

j) Contar con un Libro - Registro de Informaciones e Investigaciones bajo la custodia del Responsable del SII en los términos establecidos en el artículo 5 de este procedimiento.

k) Ofrecer información adecuada, clara y fácilmente accesible, sobre los canales internos de información y los principios esenciales del procedimiento de gestión, que en todo caso estará accesible en la página web de la Entidad, en una sección separada y fácilmente identificable.

4. DEFINICIÓN DE INFORMANTES Y OTROS USUARIOS DEL SISTEMA INTERNO DE INFORMACIÓN

La Entidad tiene diferentes colectivos de usuarios del Sistema Interno de Información: Consejeros, Directivos, socios y empleados y aquellos terceros que mantengan una relación contractual o comercial con la misma, siendo los colectivos más relevantes proveedores, subcontratistas y clientes.

A través de la Política del Sistema Interno de Información se integran en nuestro acervo normativo interno dos categorías diferenciadas de usuarios:

1. **Los informantes**: término que se recoge en la Ley 2/2023 y que identifica a las personas establecidas en su artículo 3 cuando informan sobre infracciones contempladas en el artículo 2 y aquellas otras personas de la organización que, por razón de su cargo o función, asisten, protegen, amparan o mantienen relaciones con el informante, en el ámbito del proceso de comunicación. La característica principal de los informantes es su derecho a recibir esta consideración por parte de las Autoridades Administrativas Independientes y disfrutar del régimen especial de protección establecido en la Ley 2/2023.

2. **Otros usuarios del Sistema Interno de Información:** que no pueden ser considerados informantes, tanto sea porque el contenido de la comunicación no está contemplado en el artículo 2 de la Ley como porque la relación entre comunicante y la Entidad no está contemplada en el artículo 3 de la Ley, supuestos tales como, cualquier irregularidad (error material o fraude) cometida en el proceso de emisión de Información Financiera y contable de la Entidad, infracciones del Sistema de Gobierno Interno, las violaciones del Código de Conducta. Asimismo, hay que tener en cuenta que si bien, los clientes no tienen la consideración de informantes conforme a la Ley, la Entidad habrá de gestionar las informaciones que comuniquen a la Entidad cuando las mismas impliquen una violación de la normativa interna comprendida en el ámbito material del Canal Ético.

   Sin perjuicio de ello, también hay que tener en cuenta que, respecto del colectivo de clientes, éstos cuentan con un canal específico para el planteamiento de quejas y reclamaciones a través del Servicio de Atención al Cliente (SAC) regulado en la Orden ECO/734/2004, de 11 de marzo. Este canal es susceptible de recibir indirectamente informaciones relacionadas con esta Ley. En estos casos, el responsable de este canal deberá gestionarlo dentro del SII.

En el caso de los empleados, asimismo existen vías previamente habilitadas en la Entidad para la comunicación de determinadas conductas expresamente impuestas por la normativa vigente relativas a:

1. Prevención del Blanqueo de Capitales y Financiación del Terrorismo, estableciéndose un Manual Operativo en el que se detalla el mecanismo de comunicación de conductas sospechosas de clientes al Órgano de Control Interno (OCI).

2. Acoso laboral, sexual o por razón de sexo en el que se establece un mecanismo para la comunicación de estas conductas a la Entidad.

Los canales internos habilitados en la Entidad por exigencia de normativas específicas, como son los de prevención del blanqueo de capitales o acoso laboral, sexual o por razón de sexo se integrarán en el Sistema Interno de Información respetando los requisitos derivados de la normativa que los establece, resultando este procedimiento de aplicación supletoria en lo no regulado específicamente.

En todo caso, la comunicación de conductas que pudieran ser constitutivas de acoso laboral, sexual o por razón de sexo, se llevará a cabo a través del Canal Ético de la Entidad, gestionándose de acuerdo con lo dispuesto en el presente Procedimiento y en el Protocolo de prevención y actuación del acoso sexual y acoso por razón de sexo aunque también puede comunicarse a través del correo electrónico habilitado para ello y que está indicado tanto en el Protocolo como en este Procedimiento.

El Responsable del SII y, en su caso, los gestores de los canales internos de información indicados en el apartado siguiente de este Procedimiento, asegurarán que todas las comunicaciones, informaciones, consultas, o quejas recibidas se analicen de forma independiente y confidencial, así como garantizarán la confidencialidad de la identidad de la persona que la plantea y del denunciado o denunciados, informando tan solo a las personas estrictamente necesarias en el proceso.

5. PRINCIPALES ROLES, FUNCIONES Y RESPONSABILIDADES

5.1. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN Y LOS GESTORES DEL CANAL ÉTICO.

El Consejo Rector de la Entidad, nombrará a un Responsable del Sistema Interno de Información, que deberá ser una persona física con rango de directivo o un órgano colegiado, habiendo optado la Entidad por la segunda opción. En el segundo de los casos, el Consejo Rector deberá delegar en uno de los miembros del órgano las facultades de gestión del SII y de tramitación de los expedientes de investigación. El Consejo Rector será también responsable de la destitución o cese de la persona o personas designadas.

Una vez realizados los nombramientos, deberá notificarse a la Autoridad Independiente de Protección del Informante, la designación tanto del Responsable del SII como de las personas que conforman el órgano colegiado, en su caso El plazo para realizar esta comunicación será de diez días hábiles La Entidad deberá comunicar en este mismo plazo a la Autoridad Independiente de Protección del Informante, las destituciones o ceses que se produzcan en el SII debiendo justificar los motivos del mismo.

El Responsable del SII desarrollará sus funciones de forma independiente y autónoma respecto del Consejo Rector y del resto de los órganos de la Entidad, si bien podrá compatibilizar sus funciones con el desempeño ordinario de las funciones del puesto o cargo siempre y cuando se garantice que no incurrirá en posibles situaciones de conflicto de intereses.

Entre las funciones de responsable del SII, destacan las siguientes:

- El Responsable del SII podrá elaborar, aprobar, comunicar y exigir el cumplimiento a todos los integrantes de la Entidad de cuantos procedimientos, instrucciones, formatos resulten necesarios para desarrollar y aplicar eficazmente la Política del Sistema Interno de Información y el presente procedimiento.

- El Responsable del SII podrá apoyarse en los órganos de cumplimiento que dispone la Entidad, en particular en el Órgano de Cumplimiento Penal, para gestionar el SII y en especial podrá delegar en ellos la gestión de los canales internos y/o de los procedimientos de gestión de las informaciones con la finalidad de asegurar una gestión de los canales internos eficaz, independiente y ajena a cualquier conflicto de intereses.

- Deberá mantener y custodiar un libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar en la Entidad, que no será público, quedando restringido su acceso al Responsable del SII de la Entidad que corresponda, al que únicamente podrá accederse total o parcialmente para cumplir un requerimiento razonado de una autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquella.

El responsable del SII podrá proponer al Consejo Rector la externalización de uno o todos los canales internos de información o del procedimiento de recepción de informaciones cuando considere que esa es la mejor opción para asegurar la gestión eficaz e independiente de las comunicaciones o bien sea la opción que pueda generar más confianza en los usuarios e informantes.

El procedimiento de externalización deberá asegurar en todo caso:

1. Que el tercero externo ofrece garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones.

2. Que la gestión por un tercero no comportará pérdida de las garantías y requisitos establecidos en la Política del Sistema Interno de Información, ni una delegación de la responsabilidad sobre el SII en persona distinta del Responsable del SII.

3. La consideración del tercero externo como encargado del tratamiento a efectos de la legislación sobre protección de datos personales, suscribiéndose el contrato al que se refiere el artículo 28.3 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

El responsable del SII reportará al Consejo Rector, al menos una vez al año, sobre la eficacia del SII.

El Consejo Rector de la Entidad ha designado a un órgano colegiado formado por la persona encargada del Órgano de Cumplimiento Penal y al Director General de la Entidad, nombrando como Responsable del SII al miembro del Órgano de Cumplimiento Penal, dotado de autonomía e independencia suficiente para garantizar la eficacia del Sistema y la protección de la persona informante frente a represalias por parte de cualquier miembro de la organización o ajeno a la misma. Para ello, el Consejo Rector le ha otorgado todas las facultades de decisión necesarias para ejercer esta función.

5.2. GESTIÓN DEL CANAL ÉTICO

El responsable del SII podrá contar con el soporte y apoyo de otros miembros de la Entidad:

- **Director General**: en caso de conflicto de interés o cuando se le req.

6. CANALES INTERNOS DE INFORMACIÓN

Los principios aplicables a los canales internos de información son los siguientes:

1. El SII integrará todos los canales internos que permitan la presentación de comunicaciones sobre infracciones recogidas en el artículo 2 dela Ley 2/2023..

2. El SII debe habilitar canales internos que permitan realizar comunicaciones verbales o por escrito, o de ambas formas.

3. Se habilitará también un procedimiento de comunicación mediante reuniones presenciales con los responsables del canal interno que deberá ponerse a disposición del informante en un plazo máximo de siete días a computar desde la solicitud. El Responsable del SII elaborará y aprobará dicho procedimiento que deberá tener siempre en consideración todos los requisitos establecidos en la Ley 2/2023 y en las disposiciones o recomendaciones que en su desarrollo emitan las Autoridades Administrativas de Protección a los Informantes.

4. Los usuarios de los canales internos deben ser informados de forma clara y accesible, sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

5. Los canales internos que se pongan a disposición de los usuarios e informantes deben facilitar que puedan indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones.

6. Los canales internos que permitan comunicaciones verbales, incluidas las realizadas a través de reunión presencial deberán documentar las comunicaciones, previo consentimiento del informante mediante una grabación de la conversación en un formato seguro, duradero y accesible, o a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla, ofreciendo al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

7. Los canales internos de información deben permitir la presentación y posterior tramitación de comunicaciones anónimas.

8. Los canales internos habilitados en la Entidad por exigencia de normativas específicas, como son los de prevención de blanqueo de capitales, acoso laboral, sexual o por razón de sexo, se integrarán en el Sistema Interno de Información respetando los requisitos derivados de la normativa que los establece, resultando este procedimiento de aplicación supletoria en lo no regulado específicamente.

Caja Rural Nuestra Madre del Sol pone a disposición diferentes vías de comunicación con sus grupos de interés, tanto internos como externos fomentando así una cultura de comunicación abierta, fluida y transparente.

Canales de comunicación internos:

- **Canal Ético**: herramienta online como plataforma informática especializada y accesible en la página web de la Entidad en una sección separada y accesible:

  https://cradamuz.canaletico-cajarural.com/inicio

  El Canal Ético prevé la posibilidad de emitir comunicaciones tanto anónimas como nominativas, y cuenta con medidas para preservar la seguridad e integridad de la información y tratamiento de datos personales.

- La Entidad pone a disposición tanto una dirección electrónica, denuncias.madresol@cajarural.com, como una dirección postal, a través de los cuales puede ponerse en conocimiento de la Caja cualquier consulta o irregularidad en materia penal al Órgano de Cumplimiento Penal.

- **Reunión presencial**: se ofrece la posibilidad de comunicar cualquier conducta de manera verbal mediante la petición por el informante de una reunión presencial con el Responsable del SII o en quién este delegue esta gestión.

- **Canal de protección frente a situaciones de acoso**: la Entidad cuenta con un Protocolo de prevención frente a situaciones de acoso laboral, sexual y acoso por razón de sexo, contando con una dirección a efecto de estas comunicaciones: denuncias.madresol@cajarural.com. Además de lo anterior se establece la herramienta de Canal Ético, como medio preferente para la comunicación de este tipo de situaciones.

- **Prevención de Blanqueo de Capitales y Financiación del Terrorismo**: la Entidad cuenta con un Manual de Prevención en el que se recoge que la comunicación de operaciones sospechosas se comunicarán al Órgano de Control Interno, a través de la dirección: madresol@cajarural.com. Además de lo anterior se establece la herramienta de Canal Ético, como medio preferente para la comunicación de incumplimientos de la Ley 10/2010 de Prevención de Blanqueo de Capitales y Financiación del Terrorismo.

7. CANALES EXTERNOS DE INFORMACIÓN Y AUTORIDADES ADMINISTRATIVAS DE PROTECCIÓN DEL INFORMANTE

Además de los Canales Internos de Información indicados en el apartado anterior de este procedimiento, se pone a disposición de los Informantes canales externos de comunicación gestionados por la Autoridad Independiente de Protección del Informante (A.A.I), autoridad u órganos autonómicos correspondientes, a través de los cuáles se puede informar sobre la comisión de cualesquiera de las acciones u omisiones incluidas en el ámbito de aplicación de la Ley 2/2023.

A estos efectos, el informante podrá de conformidad con el artículo 21 de la Ley 2/2023:

- Decidir si desea formular la comunicación de forma anónima o no; en este segundo caso se garantizará la reserva de identidad de la Persona informante, de modo que ésta no sea revelada a terceras personas, salvo que dicha revelación venga impuesta por ley en el marco de una investigación o proceso judicial.

- Formular la comunicación verbalmente o por escrito.

- Indicar un domicilio, correo electrónico o lugar seguro donde recibir las comunicaciones que realice la A.A.I. a propósito de la investigación.

- Renunciar, en su caso, a recibir comunicaciones de la A.A.I.

- Comparecer ante la A.A.I., por propia iniciativa o cuando sea requerido por ésta, siendo asistido en su caso, si lo considera oportuno, por abogado.

- Solicitar a la A.A.I. que la comparecencia ante la misma sea realizada por videoconferencia u otros medios telemáticos seguros que garanticen la identidad de la Persona Informante, y la seguridad y fidelidad de la comunicación.

- Ejercer los derechos que le confiere la legislación de protección de datos de carácter personal.

- Conocer el estado de la tramitación de su denuncia y los resultados de la investigación.

Tal y como establece el artículo 37 de la Ley 2/2023 las personas que comuniquen o revelen infracciones previstas en el artículo 2 a través de los procedimientos previstos accederán a las medidas de apoyo siguientes:

- Información y asesoramiento completos e independientes, fácilmente accesibles y gratuitos, sobre los procedimientos y recursos a su disponibles
- Protección frente a represalias y derechos de la persona afectada.
- Asistencia efectiva ante cualquier autoridad pertinente implicada en su protección frente a represalias, incluida la certificación de que pueden acogerse a protección al amparo de la legislación vigente.
- Asistencia jurídica en los procesos penales y en los procesos civiles transfronterizos de conformidad con la normativa comunitaria.
- Apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la A.A.I. tras la valoración de las circunstancias derivadas de la presentación de la comunicación.

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

En relación a la gestión de las comunicaciones dirigidas a los Canales externos de información, se habrá de estar a los procedimientos establecidos por la Autoridad Independiente de protección del Informante que corresponda.

8. PROCEDIMIENTO DE GESTIÓN DE LAS INFORMACIONES

8.1 Consideraciones generales

La aprobación del Procedimiento del Sistema Interno de Información es una responsabilidad del Consejo Rector, incluyéndose en este apartado los aspectos necesarios que ha de incluir conforme a la normativa vigente. Asimismo, se ha procedido a la adaptación y desarrollo conforme a lo dispuesto en la Ley 2/2023 de aquellos procesos ya establecidos en la Entidad con anterioridad a su entrada en vigor, incluyendo los procedimientos y manuales existentes en la Entidad dentro del SGCP.

El Responsable del Sistema Interno de Información, responderá de su tramitación diligente, asegurando el tratamiento adecuado de todas las comunicaciones recibidas por los gestores del Canal correspondientes.

El SII y los canales internos de información existentes deberán cumplir con todos los requisitos establecidos en la Ley 2/2023, así como las circulares o recomendaciones que pudieran publicar las Autoridades Administrativas competentes.

Todos los canales internos de información que habilite la Entidad, que se consideren, quedarán sometidos a este procedimiento.

El procedimiento debe asegurar que se pondrá a disposición de todos los usuarios de los canales de denuncia internos información clara y accesible sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

El Responsable del SII debe garantizar la confidencialidad y la protección de la persona informante en los términos establecidos en el apartado 9 del presente Procedimiento.

Los procedimientos de gestión de las comunicaciones deben salvaguardar en todo momento los derechos de la persona afectada, especialmente:

a) A que se le informe de las acciones u omisiones que se le atribuyen.

b) A ser oída en cualquier momento.

c) A que se respete su presunción de inocencia y su derecho al honor.

Dicha información a la persona afectada tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.

Se respetarán todas las disposiciones sobre protección de datos personales aplicables de acuerdo con el Título VI de la Ley 2/2023 y de conformidad con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales y el RGPD.

8.2 Fases de la gestión de las comunicaciones

A continuación, una vez recibida la comunicación a través de los canales internos habilitados para ello, se exponen cada uno de los pasos que conforman el procedimiento definido por la Entidad para la gestión de lasinformaciones:

1. Fase de comunicación: Las personas informantes podrán presentar una comunicación a través del Canal Ético disponible en la web corporativa, dirección electrónica o mediante entrevista personal, previa solicitud de la misma al Gestor del canal encargado de la recepción de la comunicación dirigiendo un correo electrónico a denuncias.madresol@cajarural.com.

El informante deberá aceptar expresamente los términos y condiciones establecidos en materia de protección de datos de carácter personal.

Cuando la comunicación se presente a través del Canal Ético, la persona informante podrá acceder a la misma mediante un Identificador y un PIN que se le asignarán al finalizar la presentación de su comunicación. Igualmente recibirá en su correo electrónico actualizaciones sobre el estado de su comunicación, cuando lo haya facilitado en el formulario de presentación de la misma.

2. Acuse de recibo: una vez recibida la comunicación por parte de la Entidad, en el plazo de siete días naturales siguientes a la recepción de cualquier comunicación deberá acusarse recibo al informante.

El Canal Ético implantado en la Entidad permite mantener una comunicación directa con la persona informante, y solicitar a esta información adicional cuando resulte oportuno.

A estos efectos, en el caso de que sea preciso completar datos, el Gestor del Canal se podrá poner en contacto con el informante a través del Canal Ético, o en su caso, a través del correo electrónico o teléfono u otro medio de contacto que el mismo haya facilitado. Cuando la comunicación sea anónima, el Canal Ético permite solicitar

información a la persona informante, pero en estos casos será necesario que ésta acceda a consultar el estado de su comunicación introduciendo el Identificador y el PIN asignado al presentar su comunicación.

En aquellos casos en los que el informante no complete la información que le sea requerida o no facilite ningún medio para contactar con él, el Gestor del Canal puede dar por concluida la gestión de la comunicación mediante su archivo. En cualquier caso, dicho archivo solo estará justificado cuando la ausencia de datos sea de tal entidad que impida al Gestor del Canal, dar trámite a la comunicación.

3. Análisis preliminar: todas las comunicaciones recibidas deberán ser objeto de un análisis preliminar por el Gestor del canal para determinar si el informante y el contenido está comprendido en el ámbito material y personal del Canal, y si procede o no procede su admisión según los criterios establecidos en la legislación vigente y en el presente procedimiento, acordándose el archivo a la mayor brevedad cuando corresponda y en el supuesto en el que dicha comunicación deba ser gestionada por el responsable de otro canal, analizar su remisión al mismo para su gestión, notificando todas estas circunstancias al informante.

Casos de supresión de la información: si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento que se tenga constancia de ello, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se conservara durante el tiempo en que se tramite el procedimiento judicial.

Casos de inadmisión: si la comunicación recibida no estuviera relacionada con acciones u omisiones que la Entidad tenga capacidad para investigar, corregir y reparar, es decir, informaciones no relacionadas con las conductas de los miembros de la Entidad o del resto de partes interesadas o socios de negocio que participan de las actividades, procesos y procedimientos de la misma, deberá inadmitirse, indicando al informante los canales internos y externos que pudieran resultar más adecuados para formular su comunicación.

4. Fase de Admisión: Cuando la comunicación haya de ser admitida, se procederá a asignar la tramitación de la misma al Gestor del canal que proceda conforme a lo dispuesto en el apartado 5 del presente procedimiento y se informará inmediatamente al Responsable del SII para poder activar los mecanismos de protección al informante.

Por último, una vez admitida a trámite, se determinará el nivel de protección que se debe asignar al informante conforme a este procedimiento.

5.Fase de investigación: tiene como finalidad realizar las actuaciones imprescindibles para determinar la naturaleza de los hechos informados y adoptar una resolución motivada sobre los mismos.

La fase de investigación deberá tramitarse con la mayor celeridad y en un plazo no superior a tres meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante, tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación.

En supuestos excepcionales y de especial complejidad se podrá extender el plazo por un periodo máximo de otros tres meses adicionales.

El Investigador deberá decidir con los medios a su alcance, sobre los siguientes aspectos:

1. Las tareas a realizar para llevar a cabo la investigación que permita tanto la preservación de las pruebas como el respeto a los derechos de los trabajadores; entrevistas personales, análisis de datos, obtención de información de fuentes externas, etc.

2. Qué departamentos o áreas deben colaborar en la investigación y a qué nivel jerárquico, dependiendo de:

a. El nivel jerárquico y número de posibles personas implicadas.

b. La necesidad de involucrar a otros departamentos para obtener datos de contraste.

3. La necesidad de solicitar, en su caso, los informes o documentos necesarios para la incoación del procedimiento a los departamentos que pudieran estar afectados por la conducta irregular.

4. La necesidad de involucrar a expertos externos para la realización de la investigación y la solicitud de los correspondientes informes periciales.

El Investigador garantizará en todo momento la confidencialidad de la investigación y el contenido del expediente, así como la confidencialidad de las personas involucradas en la investigación, actuando además conforme a lo indicado en el apartado 9 del presente procedimiento en relación a la protección del Informante.

5.Fase de Resolución:

Una vez realizadas las investigaciones oportunas, se tiene que adoptar una resolución que podrá ser:

a) De archivo de las actuaciones.

b) De remisión al órgano interno competente por la naturaleza de los hechos objeto de comunicación.

c) De remisión al Ministerio Fiscal o a la Fiscalía Europea, si procede.

El Órgano interno competente decisor será, con carácter general, el Consejo Rector, y en el caso de que la comunicación verse sobre infracciones de la normativa de Prevención de Blanqueo de Capitales, la competencia en esta fase de decisión corresponderá al Órgano de Control Interno (OCI).

Una vez adoptada la decisión final y en cumplimiento de la legislación vigente en materia de protección de datos, se procederá al archivo del expediente y la limitación de acceso al mismo. Este proceso se realizará por el Responsable del SII.

8.3 Conflictos de interés

En aquellos casos en los cuales la persona informante detecte un posible conflicto de interés con el gestor del canal que va a recepcionar y/o investigar la comunicación, o bien, es el gestor del canal quien identifica en la fase de recepción, la existencia de un posible conflicto de interés, las comunicaciones serán gestionadas por el Director General. Esto supondrá la separación de la persona en la que concurra el posible conflicto de interés, de la tramitación del expediente originado por la comunicación, en la fase del mismo en la que aquella intervenga.

En el caso de comunicaciones relativas al acoso laboral, sexual o por razón de sexo, el conflicto de interés se gestionará conforme a lo dispuesto en el Protocolo de prevención y actuación frente al acoso sexual o al acoso por razón de sexo.

Los posibles conflictos de interés pueden afectar a cualquier miembro de los establecidos en el apartado 5 de este procedimiento.

Cuando el resultado del correspondiente expediente determine que la actuación u omisión comunicada por la persona informante, realmente se ha producido y se atribuye a la persona en la que incurría el conflicto de interés, la misma se verá sometida a las mismas consecuencias que el resto del personal de la Entidad.

9. PROTECCIÓN DE LOS DENUNCIANTES

9.1. Prohibición de las represalias y protección de los informantes y personas usuarias de los canales internos

De conformidad con el artículo 36 de la Ley 2/2023 queda terminantemente prohibido cualquier acto que pueda considerarse represalia, incluidas las amenazas de represalia y las tentativas de represalia, contra las personas que presenten cualquier comunicación conforme a lo previsto en la Política del Sistema Interno de Información. Se entiende por represalia cualesquiera actos u omisiones que estén prohibidos por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, solo por su condición de informantes, o por haber realizado una revelación pública.

Los actos que tengan por objeto impedir o dificultar la presentación de comunicaciones y revelaciones, así como los que constituyan represalia o causen discriminación tras la presentación de aquellas al amparo de este procedimiento, son nulos de pleno derecho y darán lugar a medidas correctoras disciplinarias o de responsabilidad para los directivos, empleados u otras personas de la Entidad que las comentan, sin perjuicio de su comunicación a la autoridad administrativa competente para la imposición de las correspondientes sanciones.

El Responsable del SII podrá desarrollar instrucciones estableciendo criterios o directrices interpretativas sobre aquellas conductas que puedan comportar un riesgo de ser consideradas como represalias.

La protección de los usuarios de los canales de comunicación y de los informantes definidos en el artículo 4 de este procedimiento, que se encuentren dentro del ámbito material de aplicación de la norma se aplicará desde el momento del triaje inicial y admisión de su comunicación y se regirá por los siguientes criterios:

a) El Responsable del SII y los gestores del canal asegurarán la comunicación constante y fluida con el informante o usuario del canal de comunicación con la finalidad de conocer en todo momento si ha sufrido algún tipo de represalia o consecuencia tras haber realizado la comunicación.

b) Se le ofrecerá soporte y asesoramiento sobre las consecuencias de su comunicación informándoles especialmente sobre la protección que les ofrecen las Autoridades de Protección al Informante competentes y sobre los canales externos de información.

El responsable del SII actuará conforme a los procedimientos internos desarrollados al efecto, para garantizar la protección de los informantes en los términos previstos en la Ley 2/2023.

9.2. Reconocimiento y acceso al régimen de protección de los informantes y usuarios de los canales internos

Todos los usuarios del SII de la Entidad tienen derecho a la salvaguarda y confidencialidad establecidas en la Política de Sistema Interno de Información y en este procedimiento.

Las personas informantes definidas en este procedimiento tendrán derecho al régimen de protección especial previsto en la Ley 2/2023, siempre que concurran las circunstancias siguientes:

a) tengan motivos razonables para pensar que la información que transmiten es veraz en el momento de la comunicación o revelación, aun cuando no aporten pruebas concluyentes.

b) la comunicación o revelación se haya realizado siguiendo los procedimientos establecidos por la Entidad en este procedimiento y la normativa interna que lo desarrolla.

Aunque concurran los presupuestos anteriores, de conformidad con el artículo 35 de la Ley, quedan expresamente excluidos de la protección especial aquellas personas que comuniquen o revelen:

a) Informaciones contenidas en comunicaciones que hayan sido inadmitidas fundadamente por otro canal interno de información o por alguna de las causas previstas en el artículo 18.2 a) de la Ley.

b) Informaciones vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación o revelación.

c) Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores

d) Informaciones que se refieran a acciones u omisiones no comprendidas en el artículo 2 de este procedimiento.

Las personas que hayan informado de forma anónima pero que posteriormente hayan sido identificadas y cumplan las condiciones previstas en este procedimiento, tendrán derecho a la protección especial establecida en el mismo.

9.3 Derechos de las personas afectadas

Durante la tramitación de los expedientes por los Gestores del Canal, las personas afectadas por la comunicación, tendrán derecho a la presunción de inocencia, al honor, a su defensa, a acceder al expediente y ser escuchadas, así como a la protección y medidas de apoyo establecidas para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

El Responsable del SII y los Gestores del Canal le informarán de los hechos objeto de la comunicación, de su estado o cualquier información que pudiera ser relevante, salvo que las circunstancias del caso lo desaconsejen o se pueda poner en riesgo la gestión. En ningún caso la persona afectada conocerá datos que pudieran facilitar la identificación del informante.

En caso de que la comunicación sea falsa, la persona afectada tiene derecho a que así se refleje en los informes pertinentes que se realicen en el marco de la investigación.

La persona afectada tiene derecho a:

- Que la investigación y la decisión en torno a los resultados de la misma sean adoptados por personas imparciales, guiadas por la normativa que regula su funcionamiento.
- Realizar las alegaciones que considere oportunas en su defensa y proponer al respecto medios de prueba.
- Si la investigación lo permite, estar presente en el acceso a sus herramientas de trabajo, como correo electrónico o equipos informáticos, pudiendo solicitar la presencia de un representante de los empleados.

La persona afectada deberá facilitar el proceso de investigación, aportando la información que se le solicite y facilitando datos de forma veraz y, por supuesto, tendrá totalmente prohibido infligir cualquier tipo de venganza contra el informante, si conociera su identidad.

10. PROTECCIÓN DE DATOS PERSONALES

El tratamiento de datos de carácter personal en el SII atenderá en todo caso a lo previsto en la normativa de Protección de Datos de Carácter Personal, y específicamente a lo establecido en la LOPDGDD 3/2018 y en el RGPD 2016/679.

Conforme a lo previsto en dicha normativa y lo establecido en el artículo 32 de la ley 2/2023:

- No se recopilarán datos personales cuya necesidad no fuera manifiesta para tratar una información recibida, conforme a lo establecido en la Política del Sistema Interno de Información o en el presente Procedimiento. De ser recopilada por accidente, debe ser eliminada del sistema sin dilación. En ningún caso pueden ser objeto de tratamiento aquellos datos que resulten innecesarios para el conocimiento o investigación de los hechos. 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 al registro y tratamiento de los mismos.

- Cuando los datos de carácter personal sean obtenidos directamente del interesado, se les debe facilitar la información señalada en los artículos 13 y 11 del RGPD y LOPDGDD, respectivamente.

- La persona o personas a las que se refieran los hechos no recibirán información sobre la identidad del informante en base al artículo 33 de la Ley 2/2023.

- Se debe respetar el derecho al ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento y portabilidad de los datos (ARCOPOL) definidos en los artículos. 15 a 22 del RGPD, no obstante, el derecho de oposición queda excluido al existir motivos legítimos para el tratamiento.

- Queda limitada la posibilidad de acceso a los datos de carácter personal exclusivamente, y dentro de sus funciones, al Responsable del SII, a las personas encargadas de la gestión de los canales internos y procedimientos de comunicación y a aquellas otras que se designen por el Responsable del SII sin infringir las limitaciones establecidas.

- Será lícito el tratamiento de los datos de carácter personal por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas correctoras o la tramitación de procedimientos sancionadores o penales que fueran procedentes.

- Los datos de carácter personal deben ser conservados en el SII únicamente durante el tiempo imprescindible para decidir sobre la procedencia de abrir una investigación. En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, debe procederse a su supresión, salvo que la finalidad de conservación sea dejar evidencia del funcionamiento del sistema, siempre de forma anonimizada.

- Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse 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, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

- Transcurrido el plazo mencionado en el párrafo anterior, los datos podrán seguir siendo tratados, por el órgano que corresponda, en relación a la investigación de los hechos denunciados, no conservándose en el canal interno de información.

- Los empleados y terceros deberán ser informados acerca del tratamiento de datos personales en el marco de los Sistemas de información.

El Responsable del SII adoptará las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente los informantes y usuarios de los canales internos, en caso de que se hubiera identificado conforme al artículo 24 de la Ley 2/2023.

11. IMPLANTACIÓN, EVALUACIÓN Y MEJORA CONTINUA DEL SISTEMA INTERNO DE INFORMACIÓN

El SII se fundamenta en los documentos aprobados por el Consejo Rector:

- Política del Sistema Interno de Información.
- Procedimiento del Sistema Interno de Información.

Adicionalmente, el SII se basará en los siguientes elementos elaborados en la Entidad dentro del marco de Cumplimiento Normativo y en especial, en el SGCP:

1. **Identificación, evaluación y tratamiento de los riesgos** derivados del incumplimiento de la ley 2/2023 y la Política del Sistema Interno de Información, proceso integrado en el marco de análisis de riesgos de la Entidad, a través de la aplicación de la Metodología de Análisis de Riesgos de Cumplimiento Normativo.
2. Asignación clara de **roles y responsabilidades** en todas las líneas de la Entidad, de conformidad con el proceso definido en el SGCP.
3. Mantenimiento de **canales internos de información** existentes adecuados para el perfil de riesgos de la Entidad.
4. Realización de **campañas de comunicación**, incluidas en el Plan de Comunicación del SGCP.
5. Implantación de **medidas de protección de los informantes** y otros usuarios del SII.
6. Aplicación de procesos para **corregir las irregularidades** detectadas a través del SII y reparar los perjuicios ocasionados.
7. Aplicación de **medidas de diligencia debida** interna y externa en los puestos y relaciones con riesgo superior a bajo.
8. Realización de **acciones formativas y de concienciación** incluidas en los Planes de formación y concienciación adecuados para asegurar que tanto los integrantes de la Entidad como otros usuarios de los canales internos conocen y utilizan el SII.
9. Mantenimiento de **líneas de comunicación** interna y externa adecuadas para asegurar la eficacia del SII.
10. Realización de auditorías internas incluidas en los Planes de Auditoría y gestión de acciones correctivas y de mejora continua, de conformidad con el proceso definido en el SGCP.
11. Generación y custodia de evidencias de la eficacia del SII, a través de la aplicación del procedimiento de confección de procedimientos y a través de la utilización del Motor de Cumplimiento 360.
12. Realización de actividades de reporte, de conformidad con el proceso de revisión definido en el SGCP.

12. APROBACIÓN, ACTUALIZACIÓN Y MANTENIMIENTO

El presente procedimiento ha sido aprobado por el Consejo Rector de Caja Rural Nuestra Madre del Sol, que también aprobará sus actualizaciones.

Este procedimiento será revisado al menos cada dos años por el Responsable del SII.

El Responsable del SII publicará el cumplimiento de cuantas políticas, procedimientos e instrucciones sean necesarios para asegura el cumplimiento eficaz de este procedimiento, contando para alcanzar este objetivo con el apoyo y colaboración de los órganos correspondiente de la Entidad.