PROCEDIMIENTO

Sistema Interno de Información (SII)

CONTROL DE VERSIONES.

Versión	Fecha	Control
1	25/10/2023	Elaboración y aprobación 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 de Nueva Carteya 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 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 canales o procedimientos internos con finalidades propias como el de prevención de blanqueo de capitales o como el habilitado 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 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 estos.

Por todo lo anterior, el Consejo Rector de la Caja, con fecha 26 de junio de 2023, acordó la aprobación de nuestro Sistema Interno de Información, así como el órgano interno responsable 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 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 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 al órgano habilitado 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 que

   a. entren en el 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,

   b. bien 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 conforme a nuestro derecho interno 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 pudiera 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) Las violaciones del Código de Conducta de la Entidad.

f) Los incumplimientos del Protocolo para la prevención y actuación frente al acoso sexual y el 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 de Nueva Carteya es la responsable de tratamiento de los datos del sistema de información. El órgano de gobierno de la Caja -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 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.

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 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 general de gestión de las informaciones recibidas en los términos establecidos en el artículo 7 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 artículo 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, 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, las violaciones del Código de Conducta de los Directivos y Empleados.

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 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 Unidad de Recursos Humanos.

Los canales internos habilitados en la Entidad por exigencia de normativas específicas, como son los de prevención del blanqueo de capitales o acoso sexual, laboral 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.

El Responsable del SII y, en su caso, los gestores de los canales internos de información que designe, 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 SII.

El Consejo Rector de la Entidad, nombrará a un Responsable de su Sistema Interno de Información, que deberá ser una persona física con rango de directivo o un órgano colegiado. 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 de Información de Irregularidades y Protección de Informantes y el presente procedimiento.

- El Responsable del SII podrá apoyarse en los órganos de cumplimiento que dispone la Entidad 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.

5.2. GESTIÓN DEL CANAL DE DENUNCIAS

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

- Departamento de Cumplimiento Normativo: las consultas o comunicaciones que tengan que ver con las siguientes materias serán gestionadas directamente por los miembros del departamento anteriormente referido:
  - Comercialización de productos, transparencia y protección del cliente
  - Corrupción, soborno y fraude
  - Irregularidades de naturaleza financiera y contable
  - Violaciones del Código de Conducta
  - Privacidad, seguridad y confidencialidad de la información
  - Igualdad de oportunidades y no discriminación
  - Incumplimientos de la legislación o normativa interna
  - Conflicto de Interés

- Unidad de Recursos Humanos: las consultas o comunicaciones que tengan que ver con el Protocolo de Prevención del Acoso sexual y Acoso por razón de sexo serán gestionadas por los miembros de la Unidad anteriormente referida.

- Órgano de Cumplimiento Penal: cuando las consultas y denuncias recibidas versen sobre cuestiones o materias relacionadas con infracciones o delitos penales, este Órgano será el encargado de gestionarlo, quien podrá contar con el apoyo de la Unidad Técnica de Cumplimiento Penal para su tramitación.

- **Unidad Técnica de Prevención de Blanqueo de Capitales y Financiación del Terrorismo:** cuando las consultas o comunicaciones tengan que ver con incumplimientos de la Ley 2/2010, será esta Unidad la encargada de gestionarlo.

6. CANALES INTERNOS DE INFORMACIÓN

1. El SII integrará todos los canales internos que permitan la presentación de comunicaciones sobre infracciones recogidas en el artículo 2 de este procedimiento.

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.

Caja Rural de Nueva Carteya 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 de Denuncias: herramienta online como plataforma informática especializada y accesible en la página web de la Entidad en una sección separada y accesible: https://www.ruralvia.com/cms/estatico/rvia/carteya/ruralvia/es/particulares/informacion_institucional/cumplimiento-normativo/index.html

  El Canal de Denuncias 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.ncarteya@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.

- 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 hará al Órgano de Control Interno. 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.

Canales de comunicación externos:

Con carácter adicional, 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.

7. PROCEDIMIENTO DE GESTIÓN DE LAS INFORMACIONES

El presente documento tiene por finalidad definir el procedimiento para la gestión de las informaciones en la Caja, correspondiendo al Consejo Rector su aprobación.

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

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.

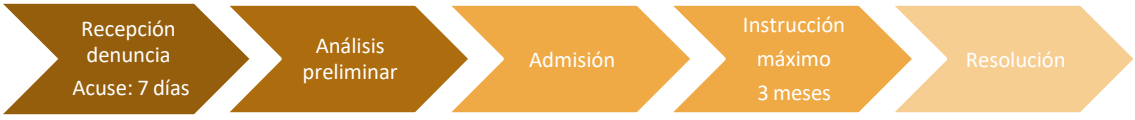
El Responsable del SII debe asegurarse que todo el personal ha recibido formación adecuada para dar respuesta a las comunicaciones de manera adecuada y ha sido advertido de la tipificación como infracción muy grave de su quebranto.

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.

Los canales cuya normativa lo requiera deberán tener mecanismos que permitan mantener la comunicación con el informante, facilitando de esta forma la solicitud de información adicional, en caso de que se considere necesario.

A continuación, se exponen cada uno de los pasos que conforman el procedimiento definido por la Entidad para la gestión de las informaciones:



1. 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, excepto en el supuesto que, por las características del canal, de la comunicación o por cualquier otra circunstancia, el

Responsable del SII o los gestores del canal consideren que el acuse de recibo pone en peligro la confidencialidad de la comunicación.

2. Análisis preliminar: todas las comunicaciones recibidas deberán ser objeto de un análisis preliminar para determinar si su contenido está comprendido en el apartado 2 de este procedimiento 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 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 denunciante.

-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.

Por último, una vez admitida a trámite, se determinará el nivel de protección que se debe asignar al informante conforme al apartado 8 de este procedimiento.

3. Procedimiento de instrucción: tiene como finalidad realizar las actuaciones imprescindibles para determinar la naturaleza de los hechos informados y adoptar una resolución.

La instrucción 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.

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.

Por último, se dará traslado al informante de la resolución del procedimiento.

El procedimiento de comunicaciones, y en general el SII, debe garantizar que cuando la comunicación sea remitida por canales de denuncia que no sean los establecidos o llegue primero a miembros del personal no responsables de su tratamiento, la comunicación será remitida inmediatamente al Responsable del SII.

El procedimiento debe respetar todas las disposiciones sobre protección de datos personales aplicables de acuerdo con el título VI de la Ley 2/2023 de Protección de Datos y Garantía de Derechos Digitales, y el RGPD.

8. PROTECCIÓN DE LOS DENUNCIANTES

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

1. 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 SII.

2. 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 cometan, sin perjuicio de su comunicación a la autoridad administrativa competente para la imposición de las correspondientes sanciones.

3. 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.

4. 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 asegurará 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 informándoseles especialmente sobre la protección que les ofrecen las Autoridades de Protección al Informante competentes y sobre los canales externos de información.

5. El Responsable del SII elaborará un procedimiento de protección al informante que asegure su salvaguarda y la confidencialidad de su identidad en todo momento.

6. El Responsable del SII podrá, en el marco del procedimiento de protección de los informantes, adoptar cuantas medidas considere adecuadas para asegurar su salvaguarda e indemnidad.

A estos efectos se entenderá por represalia la adopción de cualquier medida reactiva que implique un trato de coacción, hostilidad, discordia o aversión contra el Informante, entre otras:

- Finalización anticipada del contrato de trabajo y/o despido improcedente, cuyo origen radique en la emisión de una consulta o denuncia.
- Modificaciones perjudiciales de las funciones y responsabilidades laborales, cambios de centro de trabajo o desplazamientos no justificados.
- Tratos discriminatorios, humillantes, vejatorios, intimidantes o coercitivos durante el desempeño

profesional.

- Evaluación perjudicial del desempeño y/o negativa a la promoción laboral o salarial.

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

1. 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.

2. Las personas informantes definidas en el artículo 4 de 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.

3. Aunque concurran los presupuestos anteriores, 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.
   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.

4. 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. 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 RGPD 2016/679.

Conforme a lo previsto en dicha normativa y lo establecido en la ley 2/2023:

9.1. No se recopilarán datos personales cuya necesidad no fuera manifiesta para tratar una información recibida, conforme lo establecido en la Política de Información de Irregularidades y Protección a los Informantes 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
- Se debe respetar el derecho al ejercicio de los derechos 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 en el artículo 32 de la Ley 3/2023.
- 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 la finalidad de conservación para 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.

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.

10. 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 General del Sistema Interno de Información.

Para asegurar su eficacia, el SII deberá contar con los siguientes componentes adicionales, entre otros:

1. Asignación clara de roles y responsabilidades en todas las líneas de la Entidad.

2. Procedimientos de protección de los informantes y otros usuarios del SII que desarrollen los apartados 8 y 9.

3. Procedimientos de diligencia debida interna y externa en los puestos y relaciones con riesgo superior a bajo.

4. Procedimientos de formación, información y concienciación adecuados para asegurar que tanto los integrantes de la Entidad como otros usuarios de los canales internos conocen y utilizan el SII de la misma.

11. APROBACIÓN, ACTUALIZACIÓN Y MANTENIMIENTO

El presente procedimiento ha sido aprobado por el Consejo Rector de Caja Rural de Nueva Carteya, que también aprobará sus posibles actualizaciones.

Este procedimiento debe ser revisado cada dos años por el Responsable del SII.

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

Adicionalmente y sin que la lista sea necesariamente exhaustiva, se revisará cuando se den las siguientes circunstancias:

- Cambios en el marco normativo y/o recomendaciones del supervisor.
- Modificación de la estructura organizativa y del modelo de gobierno general de la Entidad con vinculación a este procedimiento.
- Cambios en los objetivos y estrategia de negocio o enfoque de gestión vinculados a la Política de SII.
- Desarrollo de nuevas Políticas o modificaciones sobre las existentes con impacto en este procedimiento.
- Modificaciones sustantivas en procedimientos vinculados.
- Cuando el resultado de su seguimiento y control aconseje modificar actuaciones para incrementar el grado de cumplimiento o mejorar su impacto en la Entidad o en sus empleados.