

***PROCEDIMIENTO
DEL SISTEMA INTERNO DE
INFORMACIÓN***

INDICE

0. REGISTRO	3
1. INTRODUCCION	4
2. ÁMBITO DE APLICACIÓN	4
3. ÁMBITO MATERIAL DE APLICACIÓN	4
4. PRINCIPIOS GENERALES	5
4.1. Confidencialidad	5
4.2. Prohibición de represalias	6
4.3. Protección	6
4.4. Medidas de protección frente a represalias	7
4.5. Medidas para la protección de las personas afectadas	8
4.6. La inmunidad del denunciante	8
4.7. Gestión de conflictos de interés	8
5. SISTEMA INTERNO DE INFORMACIÓN	8
6. GESTOR DEL SISTEMA INTERNO DE INFORMACIÓN	9
7. MEDIOS PARA LA COMUNICACIÓN DE DENUNCIAS	10
8. PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES	11
9. DENUNCIA DE BUENA FE Y DERECHOS DEL DENUNCIANTE	12
10.DERECHOS DEL DENUNCIADO	13
11.RECEPCIÓN, TRAMITACIÓN Y COMUNICACIÓN DE DENUNCIAS	13
12.COMUNICACION AL DENUNCIADO	15
13.FINALIZACIÓN DEL PROCESO	15
14.ARCHIVO DE LA INFORMACIÓN	16
15.PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL	16
16.COMUNICACIÓN DEL PROCEDIMIENTO	17
17.REGISTRO DE INFORMACIONES	18
18.CONDICON DE PROTECCIÓN POR REVELACIÓN PÚBLICA	18
ANEXO I	20

0. REGISTRO

Tipo de Documento:	Procedimiento del Sistema Interno de Información
Aprobado por:	Consejo de Administración
Fecha aprobación:	26.02.2026

1. INTRODUCCION

El presente Procedimiento del Sistema Interno de Información de ACACIA INVERSION, SGIIC, S.A. (en adelante la Sociedad) ha sido diseñado para promover la colaboración de todas las personas implicadas en la organización para detectar y comunicar posibles riesgos e incumplimientos en el seno de la actividad e impulsar el buen gobierno corporativo.

La Sociedad debe de disponer de mecanismos para la prevención, detección y reacción ante delitos. Dicha referencia viene recogida en el Código Penal artículo 31 bis y concordantes de la L.O. 1/2015 y 1/2019 de modificación del Código Penal), en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (Art.63), en el Dictamen 1/2006 del grupo del artículo 29 (protección de datos de carácter personal), en el su Dictamen 1/2006 (Art. 32) y en 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.

Las personas implicadas en la Organización deben disponer de una cultura de cumplimiento y de gobierno corporativo y a través de la comunicación de posibles infracciones contribuir a mejorar los procedimientos.

Este procedimiento es compatible con el procedimiento de “Abuso de mercado” y el Manual de Prevención del blanqueo de capitales y financiación del terrorismo.

2. ÁMBITO DE APLICACIÓN

El procedimiento será de aplicación a todos los directivos y empleados, proveedores, clientes, cualesquiera que actúen en nombre y/o por cuenta de la Sociedad y deberán comunicar, a través del Sistema Interno de Información, cualquier irregularidad de las que tengan conocimiento.

3. ÁMBITO MATERIAL DE APLICACIÓN

La Ley protege a las personas físicas que informen, de:

- √ Cualesquiera acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea siempre que:
 - Estén 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, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno;

- 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); 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.
- √ Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave. En todo caso, se entenderán comprendidas todas aquellas infracciones penales o administrativas graves o muy graves que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.
 - √ Incumplimientos de las normas de conducta.
 - √ Utilización de información privilegiada.
 - √ Procedencia ilícita de fondos constitutiva de una posible infracción de lo establecido en la normativa de blanqueo de capitales.
 - √ Revelación de información confidencial de toda índole.
 - √ Prácticas tipificadas como abuso de mercado.
 - √ Otras acciones que puedan perjudicar el buen nombre de la Sociedad o al personal o a terceros.

4. PRINCIPIOS GENERALES

4.1. Confidencialidad

El procedimiento de comunicación debe cumplir con la normativa en materia de protección de datos y debe garantizar que la identidad de los empleados, directivos o personas que informen de las infracciones cometidas en la Sociedad no sea revelada a terceros.

La denuncia podrá ser anónima. Como medida para garantizar dicha confidencialidad se hace constar expresamente que el ejercicio del derecho de acceso por parte del denunciado no supone, en ningún caso, el acceso a los datos relativos a la identidad del denunciante. No obstante, si por necesidad para la investigación y conclusión fuese necesario identificar a la persona denunciante, las personas que tengan acceso a dicha información, deberán mantener el deber de confidencialidad. No será de aplicación si, a la hora de comunicar a través del

Sistema Interno de Información cualquier irregularidad detectada, el denunciante se identificara.

La obligación de comunicaciones o denuncias internas no sustituye la necesaria existencia de mecanismos específicos e independientes de comunicación interna de operaciones sospechosas conforme a lo previsto en los artículos 18 y 63 de la Ley 10/2010 de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo ni en lo previsto en el artículo 32 del Reglamento (UE) nº 596/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre el abuso de mercado (Reglamento sobre abuso de mercado) y por el que se derogan la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, y las Directivas 2003/124/CE, 2003/125/CE y 2004/72/CE de la Comisión.

4.2. Prohibición de represalias

Se prohíben expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación conforme a lo previsto en esta ley.

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.

La persona que viera lesionados sus derechos por causa de su comunicación o revelación una vez transcurrido el plazo de dos años, podrá solicitar la protección de la autoridad competente que, excepcionalmente y de forma justificada, podrá extender el período de protección, previa audiencia de las personas u órganos que pudieran verse afectados. La denegación de la extensión del período de protección deberá estar motivada.

Los actos administrativos 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 esta ley, serán nulos de pleno derecho y darán lugar, en su caso, a medidas correctoras disciplinarias o de responsabilidad, pudiendo incluir la correspondiente indemnización de daños y perjuicios al perjudicado.

4.3. Protección

Las personas que comuniquen o revelen infracciones tendrán derecho a protección siempre que concurren las circunstancias siguientes:

- √ tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación o revelación, aun cuando no aporten pruebas concluyentes, y que la citada información entra dentro del ámbito de aplicación de esta ley,

- √ la comunicación o revelación se haya realizado conforme a los requerimientos previstos en este procedimiento.

No gozarán de protección aquellas personas que comuniquen o revelen:

- √ Informaciones contenidas en comunicaciones que hayan sido inadmitidas por algún canal interno de información o por alguna de las siguientes causas:
 - Cuando los hechos relatados carezcan de toda verosimilitud.
 - Cuando los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico incluida en este procedimiento.
 - Cuando la comunicación carezca manifiestamente de fundamento o existan indicios racionales de haberse obtenido mediante la comisión de un delito.
 - Cuando la comunicación no contenga información nueva y significativa sobre infracciones en comparación con una comunicación anterior respecto de la cual han concluido los correspondientes procedimientos, a menos que se den nuevas circunstancias de hecho que justifiquen un seguimiento distinto.
- √ 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.
- √ Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores.
- √ Informaciones que se refieran a acciones u omisiones no comprendidas en el apartado de ámbito material de aplicación de este procedimiento.

No obstante, las personas que hayan comunicado o revelado públicamente información sobre acciones u omisiones de forma anónima pero que posteriormente hayan sido identificadas y cumplan las condiciones previstas en esta ley, tendrán derecho a la protección que la misma contiene.

4.4. Medidas de protección frente a represalias

No se considerará que las personas que comuniquen información sobre las acciones u omisiones o que hagan una revelación pública de conformidad con este procedimiento hayan infringido ninguna restricción de revelación de información, y aquellas no incurrirán en responsabilidad de ningún tipo en relación con dicha comunicación o revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública de dicha información era necesaria para revelar una acción u omisión.

Los informantes no incurrirán en responsabilidad respecto de la adquisición o el acceso a la

información que es comunicada o revelada públicamente, siempre que dicha adquisición o acceso no constituya un delito.

4.5. Medidas para la protección de las personas afectadas

Durante la tramitación del expediente las personas afectadas por la comunicación tendrán derecho a la presunción de inocencia, al derecho de defensa y al derecho de acceso al expediente en los términos regulados en esta ley, así como a la misma protección establecida para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

4.6. La inmunidad del denunciante

Cuando el denunciante hubiera obtenido de manera legal acceso a la información comunicada o los documentos que la contienen, tendrá inmunidad con relación a la responsabilidades civil, administrativa o laboral derivada de la denuncia presentada.

Esto se aplica tanto a los casos en los que el denunciante revele el contenido de documentos a los que tenga acceso legalmente como a aquellos en los que realice copias de los mismos o los retire de los locales de la organización de la cual es empleado en contravención de cláusulas contractuales o de otro tipo que estipulen que dichos documentos son propiedad de la organización.

Cuando el denunciante haya obtenido la información o documentos mediante la comisión de una infracción penal como la intromisión física o informática, su responsabilidad penal ha de regirse por la legislación que en cada caso sea aplicable.

No obstante, lo anterior, el denunciante será responsable de las acciones y omisiones que no guarden relación con la denuncia o no resulten necesarias para revelar una infracción.

4.7. Gestión de conflictos de interés

Cuando uno de los participantes en el proceso de investigación se vea afectado al presentar una denuncia, debe ser excluido completamente del procedimiento, tanto de la fase de investigación como el análisis y la resolución. Los miembros excluidos, no importa si son del consejo de administración o del comité de dirección, están obligados a mantener la confidencialidad de la denuncia y se les prohíbe el acceso a información sensible, como la identidad del denunciante o detalles sobre el proceso de investigación en curso.

5. SISTEMA INTERNO DE INFORMACIÓN

El canal interno deberá permitir realizar comunicaciones por escrito o verbalmente, o de las dos formas. La información se podrá realizar bien por escrito, a través de correo postal o a través de

cualquier medio electrónico habilitado al efecto, o verbalmente, por vía telefónica o a través de sistema de mensajería de voz. A solicitud del informante, también podrá presentarse mediante una reunión presencial dentro del plazo máximo de siete días.

En su caso, se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo a lo que establece la normativa relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Además, a quienes realicen la comunicación a través de canales internos se les informará, 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.

Al hacer la comunicación, el informante podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones.

Las comunicaciones verbales, incluidas las realizadas a través de reunión presencial, telefónicamente o mediante sistema de mensajería de voz, deberán documentarse de alguna de las maneras siguientes, 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.

Sin perjuicio de los derechos que le corresponden de acuerdo a la normativa sobre protección de datos, se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

Debe permitir la presentación y posterior tramitación de comunicaciones anónimas.

6. GESTOR DEL SISTEMA INTERNO DE INFORMACIÓN

El órgano de administración designará la persona física responsable de la gestión de dicho canal interno, y de su destitución o cese.

Debe ser un directivo de la entidad, que ejercerá su cargo con independencia del órgano de administración o de gobierno de la misma. Atendiendo al principio de proporcionalidad, el Directivo podrá realizar el desempeño ordinario de sus funciones del puesto o cargo con las de Responsable del Canal, tratando en todo caso de evitar posibles situaciones de conflicto de interés.

Si el Responsable del Canal es un órgano colegiado, este debe delegar en uno de sus miembros las facultades de gestión del canal y de tramitación de expedientes de investigación.

El Presidente de la Sociedad es el gestor del Canal de Denuncias. Será quien reciba y valore todas las comunicaciones y/o denuncias que se informen a través de este medio.

7. MEDIOS PARA LA COMUNICACIÓN DE DENUNCIAS

El denunciante siempre tendrá la capacidad de determinar si pretende efectuar una comunicación o denuncia de llevarla a cabo de forma confidencial o anónima.

El denunciante debe poder elegir el cauce de denuncia más adecuado en función de las circunstancias particulares del asunto. No obstante, se recomienda, que las denuncias se comuniquen a través de una triple vía, a elección del denunciante:

- √ Mediante correo electrónico a la siguiente dirección: canal.denuncias.interno@acacia-inversion.com deberá utilizar obligatoriamente el formulario de comunicación o denuncia que se adjunta en el presente Procedimiento como Anexo I, y que estará a disposición en la página web de la Empresa.
- √ A través del formulario habilitado para comunicar cualquier incidencia, al cual se accederá mediante el siguiente link:

[Formulario Sistema Interno de Información](#)
- √ Si el denunciante optara por la comunicación mediante correo ordinario, deberá utilizar obligatoriamente el formulario de comunicación o denuncia que se adjunta en el presente Procedimiento como Anexo I, y que estará a disposición en la página web de la Empresa.
- √ Comunicación verbal: en este caso, la Sociedad advertirá que la conversación será grabada y que sus datos personales serán tratados conforme a lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre.
- √ A solicitud del denunciante, también podrá presentarse mediante una reunión presencial, dentro del plazo máximo de siete días.
- √ Además de los anteriores cauces citados, el denunciante dispone de un canal externo adicional que es el canal de denuncias habilitado por la CNMV. En caso de optar por este canal, deberá dirigir su denuncia utilizando cualquiera de los canales establecidos en la página web de la CNMV.

No se admitirá ninguna comunicación o denuncia fuera de estos cauces, pudiéndose proceder a su rechazo y destrucción sin necesidad de trámite alguno o de comunicación, salvo que excepcionalmente así lo determine el Consejo de Administración de la Sociedad.

En todo caso, en el funcionamiento del Canal de Comunicaciones y/o Denuncias se incluirá información clara y fácilmente accesible sobre los procedimientos de denuncia externa ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

En el presente caso, el Canal de Comunicaciones y/o denuncias está diseñado, establecido y gestionado de manera segura, a los efectos de garantizar la confidencialidad de la identidad del denunciante y cualquier tercero mencionado en la comunicación o denuncia este suficientemente protegido, impidiéndose el acceso a ella al personal no autorizado

8. PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES

El procedimiento contiene principios siguientes:

- √ Identificación del canal o canales internos de información a los que se asocian.
- √ Inclusión de 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.
- √ Envío de acuse de recibo de la comunicación al informante, en el plazo de siete días naturales siguientes a su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.
- √ Determinación del plazo máximo para dar respuesta a las actuaciones de investigación, que no podrá ser superior a tres meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante, a tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, este podrá extenderse hasta un máximo de otros tres meses adicionales.
- √ Previsión de la posibilidad de mantener la comunicación con el informante y, si se considera necesario, de solicitar a la persona informante información adicional.
- √ Establecimiento del derecho de la persona afectada a que se le informe de las acciones u omisiones que se le atribuyen, y a ser oída en cualquier momento. Dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.
- √ Garantía de la confidencialidad cuando la comunicación sea remitida por canales de denuncia que no sean los establecidos o a miembros del personal no responsable de su tratamiento, al que se habrá formado en esta materia y advertido de la tipificación como infracción muy grave de su quebranto y, asimismo, el establecimiento de la obligación del receptor de la comunicación de remitirla inmediatamente al Responsable del Sistema.
- √ Exigencia del respeto a la presunción de inocencia y al honor de las personas afectadas.
- √ Respeto de las disposiciones sobre protección de datos personales de acuerdo a lo previsto en el título VI.
- √ Remisión de la información al Ministerio Fiscal con carácter inmediato cuando los hechos

podrían ser indiciariamente constitutivos de delito. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

9. DENUNCIA DE BUENA FE Y DERECHOS DEL DENUNCIANTE

Tendrá la consideración de denuncia de buena fe aquella tramitada conforme a lo establecido en el presente procedimiento, cuando ponga en conocimiento una serie de hechos o indicios de apariencia irregular, ilícita o delictiva, actuando en la creencia racional de que los hechos o indicios relacionados son ciertos.

Los denunciantes que actúen de buena fe conforme a las disposiciones del presente Reglamento no podrán ser sancionados disciplinariamente, despedidos o apartados de su función, ni podrán sufrir perjuicio alguno en su relación con la Sociedad como consecuencia de la interposición de una denuncia.

La interposición de una denuncia de buena fe conforme a las disposiciones del presente Reglamento no podrá tener, en ningún caso, la consideración de infracción del Código de Conducta, de los valores éticos de la Sociedad, ni de cualquier obligación asumida de forma contractual.

El denunciante de buena fe tendrá derecho a ser informado, en cualquier momento, del estado de tramitación de su denuncia, así como del resultado de la misma.

La identidad del denunciante de buena fe no será revelada ni a terceros ni a la propia organización. Solo en caso de estricta necesidad, y mediando el consentimiento de la persona denunciante, podrán revelarse a la Sociedad sus datos de identificación. El gestor del Sistema Interno de Información, previa solicitud por escrito por parte de la Sociedad, analizará la situación objetiva de necesidad de revelar la identidad del denunciante, y, en caso coincidir en la necesidad, contactará con el denunciante para solicitar su consentimiento. Los datos de carácter personal que se revelen podrán ser utilizados por la Sociedad a los únicos efectos de solventar la situación de necesidad, y serán debidamente destruidos una vez haya cesado tal situación.

El tratamiento de los datos del denunciante se basa en su consentimiento. No obstante, tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. El denunciante puede ejercer sus derechos de acceso, rectificación, supresión, limitación y oposición al tratamiento de sus datos personales a través de la dirección de correo electrónico dpd@acacia-inversion.com en aplicación del Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

La Sociedad podrá adoptar las correspondientes medidas disciplinarias que sean procedentes,

cuando la investigación interna determine que la comunicación realizada es falsa, y que la persona que la ha realizado es consciente de su falsedad.

10.DERECHOS DEL DENUNCIADO

La persona denunciada tendrá derecho a conocer la existencia de la denuncia. La Sociedad se obliga a informar de la existencia de una denuncia en su contra en un plazo máximo de tres meses desde la recepción del informe por parte del gestor del Sistema Interno de Información.

En el caso de que la denuncia acabe siendo archivada, bien por no haber tenido lugar los hechos descritos, bien por no ser estos irregulares, ilícitos o delictivos, el denunciado tendrá derecho a que así conste en el oportuno expediente y Registro de denuncias.

La protección de los datos de los denunciados será garantizada en el tratamiento. Su tratamiento está basado en el interés legítimo perseguido por la Sociedad como responsable del tratamiento de mantener un programa de denuncia de irregularidades.

11.RECEPCIÓN, TRAMITACIÓN Y COMUNICACIÓN DE DENUNCIAS

Cada denuncia interpuesta conforme al presente Reglamento tendrá asignada un código único para su identificación, y será debidamente almacenada en el Registro de denuncias.

Se realizará un análisis preliminar sobre los hechos denunciados y el material probatorio adjunto, y procederá a la calificación jurídica de los mismos. Dicha calificación se acompañará de una serie de recomendaciones dirigidas a la Sociedad sobre el debido proceder para cada una de las denuncias recibidas.

El gestor del Sistema Interno de Información remitirá el Registro de denuncias al Consejo de Administración de la Sociedad, sin incluir, en ningún caso, los datos personales de los denunciantes. Cuando los hechos relacionados en una denuncia revistan especial gravedad, el gestor del Sistema Interno de Información remitirá con la máxima celeridad un informe.

Recibido el Registro de denuncias, la Sociedad procederá a la apertura de un expediente por cada una de las denuncias registradas, cuyo código de identificación coincidirá con el código de identificación de la denuncia.

El Consejo de Administración de la Sociedad, tras valorar la denuncia, su calificación y las recomendaciones adjuntas, adoptará una decisión respecto de cada expediente, que podrá consistir en la apertura de una investigación o en el archivo del expediente, cuando la denuncia fuera totalmente infundada. En cualquiera de los casos, dejará constancia en el expediente de las razones que motivan la decisión adoptada.

La Sociedad adoptará, en su caso, las medidas cautelares oportunas para evitar la reiteración de los hechos denunciados durante el procedimiento de investigación y para asegurar los

medios probatorios que puedan obtenerse.

La Sociedad velará por el respeto a los derechos reconocidos a los denunciantes, a los denunciados y a terceras personas que puedan verse implicadas en la denuncia.

El plazo para la tramitación del expediente, investigación y resolución no podrá exceder de tres meses a contar desde su apertura o, si no se remitió un acuse de recibo al informante, a tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, este podrá extenderse hasta un máximo de otros tres meses adicionales.

Enviaré un acuse de recibo de la comunicación al informante, en el plazo de siete días naturales siguientes a su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación, se le comunicará las medidas previstas o adoptadas para tramitar la denuncia y los motivos de dicha tramitación.

En todos los casos, el denunciante será informado de los progresos y el resultado de la investigación.

Si la comunicación presentara deficiencias en la comunicación y/o denuncia, el gestor lo comunicará al denunciante este hecho. Si en el plazo de 5 días hábiles a contar desde el día siguiente al de la notificación, no se subsanaran los requerimientos, se procederá a la inadmisión de la denuncia y a su consiguiente archivo, no iniciándose, por tanto, una investigación.

El Gestor del Canal evidenciará la recepción de la comunicación y/o denuncia, de la decisión adoptada y de su archivo, haciéndose constar los motivos en los que se haya basado para adoptar tal decisión.

Esta resolución del Gestor del Canal no impedirá la iniciación posterior de una investigación si se recibiera información de carácter adicional a la ya valorada.

En todo supuesto de inadmisión, el Gestor del Canal procederá a informar al denunciante, por escrito y en la dirección de contacto por él facilitada, de la decisión de inadmisión, indicando y motivando suficientemente la causa de inadmisión que concurra.

Adicionalmente, en el transcurso de cualquier investigación, se le podrá pedir al denunciante que proporcione información adicional, pero éste no tendrá la obligación de hacerlo. Asimismo, cuando todavía se esté considerando la tramitación apropiada, el denunciante será informado de ello, así como de cualquier otra respuesta que deba esperar.

El expediente quedará cerrado con la realización de la notificación. El denunciante podrá aportar aquella información que considere oportuna, a efectos de volver a abrir el expediente.

Durante la fase de análisis el gestor está habilitado para solicitar al denunciante cuanta información precise. Adicionalmente, en el transcurso de cualquier investigación, se le podrá pedir al denunciante que proporcione información adicional.

Si la comunicación y/o denuncia no cumple con los requisitos de forma exigidos, o los hechos comunicados no suponen una infracción de las previstas en el ámbito objetivo del Canal de Denuncias, se comunicará al denunciante su inadmisión, y con relación a los datos personales contenidos en ella, se eliminarán de manera inmediata, de acuerdo con las causas de inadmisibilidad de las comunicaciones y/o denuncias previstas en el presente apartado.

Son causas de inadmisión entre otras:

- √ Las comunicaciones y/o denuncias que se reciban por cauces distintos a lo establecido en esta Política del Canal de Denuncias.
- √ El incumplimiento de los requisitos de forma exigidos.
- √ Cuando los hechos denunciados no tengan encaje en el alcance objetivo del Canal de Denuncias.
- √ Cuando se produzca la descripción de los hechos de forma genérica, imprecisa o inconcreta.
- √ Cuando la comunicación realizada se refiera a hechos que nada tengan que ver con la Empresa.

Las denuncias que sean una mera repetición de la anterior no serán admitidas.

12.COMUNICACION AL DENUNCIADO

Sin perjuicio de la confidencialidad de la identidad del denunciante, la persona denunciada será informada de la existencia de la denuncia, de los hechos de los que se le atribuyen, los departamentos y servicios que tengan acceso al informe y de la posibilidad de ejercer los derechos sobre protección de datos, de conformidad con la normativa vigente sobre la misma.

No obstante, cuando exista un riesgo importante de que dicha notificación pusiera en peligro la capacidad para investigar de manera eficaz la alegación o recopilar las pruebas necesarias, la notificación a la persona inculpada podría demorarse mientras exista dicho riesgo.

13.FINALIZACIÓN DEL PROCESO

Una vez finalizada la investigación o el plazo para llevar a cabo el análisis, el gestor comunicará por escrito al Consejo de Administración de la Sociedad el resultado de la misma, así como las medidas que deben adoptarse con motivo de la denuncia. El gestor del Sistema Interno de Información pondrá en conocimiento del denunciante, de forma inmediata, dicha resolución.

En caso de acreditarse los hechos que traen causa la denuncia, la resolución especificará las sanciones a imponer a la persona o personas denunciadas, así como las medidas a adoptar

para evitar que los hechos vuelvan a producirse.

El gestor verificará que se apliquen las sanciones o medidas propuestas en cada caso.

La ejecución de dichas sanciones o medidas se llevará a cabo por la persona o personas que tengan atribuidas dichas funciones en la Sociedad.

Resuelta la denuncia y notificada su resolución, los datos de identificación de denunciante y denunciado serán definitivamente suprimidos del Registro de Denuncias.

14. ARCHIVO DE LA INFORMACIÓN

En cuanto a la gestión y archivo tanto de los datos personales como de toda la información facilitada por el Denunciante, serán tratados garantizando que serán de acceso restringido, y estarán protegidos por las medidas de seguridad adecuadas de acuerdo con la legislación vigente en materia de protección de datos.

Los datos de quien formule la comunicación, en el caso de que se hubiera identificado, y de los empleados y terceros únicamente se conservarán en el sistema de denuncias durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

En todo caso, transcurridos tres meses desde la introducción de los datos, se procederá a su supresión del registro de denuncias, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica debiendo conservarse en un sistema distinto del propio de denuncias internas.

15. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Los datos personales recabados en el marco del procedimiento del Sistema Interno de Información serán tratados con la exclusiva finalidad de tramitar las comunicaciones y/o denuncias al amparo del artículo 24 de la Ley Orgánica 3/2018 de 5 de diciembre, a los efectos de gestionar y, en su caso, investigar la realidad de los hechos objeto de la comunicación y/o denuncia.

Aquellos datos personales que se recaben en el marco de una comunicación y/o denuncia y que den lugar a la apertura de la correspondiente investigación se integrarán en el tratamiento denominado “Sistema Interno de Información”, respecto del que la Empresa ostenta la condición de responsable del tratamiento.

El responsable del tratamiento debe tomar y aplicar las medidas de seguridad necesarias para garantizar la confidencialidad, integridad y disponibilidad de los datos personales obtenidos y tratados a través del Sistema Interno de Información.

En cuanto a la confidencialidad, se hace especial hincapié en la necesidad de preservar y garantizar la confidencialidad de los datos personales del denunciante, en el caso de que la denuncia no fuera anónima. De igual forma se garantiza la anonimidad del sujeto en caso de denuncia anónima, en todos los aspectos, de identidad y de rastreo (cookies/rastreo IP).

En el caso de los datos personales contenidos en aquellas comunicaciones y/o denuncias que no sean admitidas a trámite, no se incorporarán a ningún tratamiento, procediéndose a su eliminación o borrado seguro con carácter inmediato o solamente podrán constar de forma anonimizada.

Tanto el denunciante como el denunciado serán informados debidamente, en cada caso, de las personas y órganos concretos a los cuales se van a comunicar sus datos personales.

El acceso a los datos contenidos en el Registro de Denuncias quedará limitado exclusivamente al gestor, a los encargados del tratamiento que se designen a tal efecto y a abogados cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales.

Una vez transcurridos tres meses desde la introducción de los datos de la denuncia, deberá procederse a su supresión del sistema, con la excepción que permite conservarlos para dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la Sociedad. Transcurrido este plazo, los datos podrán seguir siendo tratados por el órgano al que corresponda la investigación de los hechos denunciados, pero no podrán conservarse en el propio sistema de información de denuncias y se conservarán durante el tiempo necesario, con un plazo máximo de 10 años.

Los interesados podrán ejercitar sus derechos de acceso, rectificación, cancelación y oposición y cualesquiera otros derechos previstos en la normativa vigente sobre protección de datos personales, a través de la dirección de correo electrónico dpd@acacia-inversion.com adjuntando una copia de un documento oficial que pruebe su identidad.

No obstante, lo anterior, el derecho de acceso del denunciado estará limitado a sus propios datos de carácter personal, no teniendo acceso a los datos sobre la identidad del denunciante dado el carácter confidencial de dichos datos vinculados al Sistema Interno de Información, ni a otros datos personales de terceros obrantes en el expediente.

16.COMUNICACIÓN DEL PROCEDIMIENTO

Los empleados y demás personas físicas o jurídicas vinculados a la Sociedad deberán estar informados de la existencia del Sistema Interno de Información y del tratamiento de los datos que conlleva la formulación de una denuncia. Para ello, la Sociedad deberá circularizar el procedimiento a todas las partes vinculadas y dejar constancia documental de su recepción por parte de las mismas.

En caso de contar con una página web, dicha información deberá constar en la página de inicio,

en una sección separada y fácilmente identificable.

17. REGISTRO DE INFORMACIONES

La Sociedad contar con un libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad previstos en este procedimiento y en la ley que resulta de aplicación.

Este registro no será público y únicamente a petición razonada de la Autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquella, podrá accederse total o parcialmente al contenido del referido registro.

Los datos personales relativos a las informaciones recibidas y a las investigaciones internas a solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con esta ley. En particular, se tendrá en cuenta:

- √ 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.

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.

- √ En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, 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 podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

En ningún caso podrán conservarse los datos por un período superior a diez años.

18. CONDICION DE PROTECCIÓN POR REVELACIÓN PÚBLICA

La persona que haga una revelación pública podrá acogerse a protección en virtud de esta ley si se cumplen las condiciones de protección en los principios generales de este procedimiento y alguna de las condiciones siguientes:

- √ Que haya realizado la comunicación primero por canales internos y externos, o directamente por canales externos, sin que se hayan tomado medidas apropiadas al respecto en el plazo establecido.
- √ Que tenga motivos razonables para pensar que, o bien la infracción puede constituir un peligro inminente o manifiesto para el interés público, en particular cuando se da una situación de emergencia, o existe un riesgo de daños irreversibles, incluido un peligro para la integridad física de una persona; o bien, en caso de comunicación a través de canal externo de información, exista riesgo de represalias o haya pocas probabilidades de que se dé un tratamiento efectivo a la información debido a las circunstancias particulares del caso, tales como la ocultación o destrucción de pruebas, la connivencia de una autoridad con el autor de la infracción, o que esta esté implicada en la infracción.

Las condiciones para acogerse a protección previstas en el apartado anterior no serán exigibles cuando la persona haya revelado información directamente a la prensa con arreglo al ejercicio de la libertad de expresión y de información veraz previstas constitucionalmente y en su legislación de desarrollo.

ANEXO I

FORMULARIO DE COMUNICACIÓN DE DENUNCIAS

A través de este canal de denuncias, usted podrá notificar de forma confidencial y/o anónima las potenciales conductas inapropiadas o sospechosas de las que tenga conocimiento dentro del seno de la Sociedad.

Al enviar este documento el Denunciante presta expresamente su consentimiento a los efectos del tratamiento de sus datos personales por parte de ACACIA INVERSIÓN SGIIC, S.A., con la finalidad indicada en el mismo.

*** Obligatorio**

1. ¿Trabaja usted en la Entidad? *

- ☐ Sí
- ☐ No

2. Asunto de la denuncia. *

- ☐ Blanqueo de Capitales y Financiación del Terrorismo
- ☐ Abuso de mercado
- ☐ Protección de datos personales
- ☐ Otros

3. Descripción de los hechos que motivan la denuncia. *

4. Información de contacto.

(Nombre / Apellidos / Teléfono / Email)