

POLÍTICA

CANAL DE DENUNCIAS

ADARA VENTURES, SGEIC, S.A.

POL 05 · Aug 2026

ÍNDICE

1. OBJETO.....	3
2. ÁMBITO DE APLICACIÓN	3
3. RESPONSABILIDADES GENERALES.....	3
4. MEDIOS PARA REALIZACIÓN DE LAS COMUNICACIONES	4
5. TRAMITACIÓN DE LAS COMUNICACIONES	4
5.1 Recepción y registro de la comunicación.....	4
5.2 Trámite de admisión.....	5
5.3 Investigación	5
5.4 Terminación de las actuaciones.....	5
6. COMUNICACIÓN DE DENUNCIAS FALSAS O DE MALA FE.....	6
7. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.....	6
8. LEGISLACIÓN VIGENTE	7
Anexo I Tipología de casos.....	8

1. OBJETO

La presente política ha sido desarrollada por ADARA VENTURES, SGEIC, SA (en adelante la "Sociedad") con el objetivo de detallar el procedimiento seguido en el canal de denuncias interno desarrollado en cumplimiento, entre otras disposiciones normativas, del art. 8 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.

El objetivo del Canal de Denuncias es que empleados, clientes, proveedores y terceras personas relacionadas con la Sociedad o su actividad puedan comunicar cualquier acto que haya podido suceder en la Sociedad y que pueda suponer una infracción, un delito o una vulneración de nuestros procedimientos internos, entre otros:

- Infracción de la normativa de PBC/FT
- Infracción de la normativa de LOPD
- Infracción de la normativa de Abuso de Mercado
- Reglamento Interno de Conducta

El Canal de denuncias de la Sociedad es accesible a través de la web corporativa: <https://www.adara.vc/cumplimiento-normativo> o bien desde el canal interno en la URL: [Canal de Denuncias](#), permitiéndose su uso a personas que tengan conocimiento de posibles riesgos de infracciones administrativas y/o penales de gravedad atribuibles a cualquier persona o entidad vinculada al grupo en su esfera profesional.

Este Canal facilita la formulación segura de las comunicaciones asegurando que durante todo el proceso se garantice eficazmente la protección de la privacidad de las personas involucradas y la confidencialidad sobre los datos contenidos en la denuncia, pudiendo realizarse la denuncia de forma anónima si así lo considera el denunciante.

2. ÁMBITO DE APLICACIÓN

La presente política va destinada a los empleados, clientes, proveedores y terceras personas involucradas en la actividad de la Sociedad que pudieran hacer uso del Canal de Denuncias conforme a lo detallado en la misma.

Todos los directivos y empleados, con independencia de cuál sea la modalidad jurídica que determine su relación laboral o de servicios, proveedores, patrocinadores, colaboradores, agentes, miembros de los diferentes órganos colegiados de la Empresa deberán comunicar, a través del Canal de Denuncias, cualquier irregularidad o incumplimiento de los que tengan conocimiento y que estén incluidos en su ámbito objetivo, sin el temor a ser objeto de despido, o de cualquier otro tipo de represalia, y, con la seguridad de que la información proporcionada será tratada con la más absoluta confidencialidad.

El Canal de denuncias debe entenderse como un instrumento que permita la comunicación de irregularidades o incumplimientos. Por ello, no debe emplearse de manera indiscriminada, sino para los fines que ha sido concebido.

3. RESPONSABILIDADES GENERALES

Se indican a continuación las responsabilidades generales respecto del Canal de Denuncias:

- Consejo de Administración: Aprobación de la presente Política y sus sucesivas actualizaciones. Dotar de los medios necesarios a la Sociedad para el correcto funcionamiento del Canal.
- Unidad de Control: Actualización de la presente política.
- Responsable del sistema: Funcionamiento del canal de denuncias. Garantizar la confidencialidad de las personas denunciantes, en su caso. Registro de las denuncias. Conservación de la documentación.
- Órgano de Control Interno en materia de PBC/FT: Apoyo al Órgano de prevención de riesgos penales en las denuncias referentes a incumplimientos de la Ley de PBC/FT.
- Órgano de Seguimiento del RIC: Apoyo al Órgano de prevención de riesgos penales en las denuncias referentes a incumplimientos del Reglamento Interno de Conducta de la Sociedad y de la normativa en materia de Abuso de Mercado.
- Responsable de seguridad en materia de LOPD: Apoyo al Órgano de prevención de riesgos penales en las denuncias referentes a incumplimientos de la normativa en materia de protección de datos.

4. MEDIOS PARA REALIZACIÓN DE LAS COMUNICACIONES

El Sistema interno de información debe utilizarse de manera preferente para canalizar la información, pues una actuación diligente y eficaz en el seno de la Sociedad podría paralizar las consecuencias perjudiciales de las actuaciones investigadas.

No obstante, declarada esta preferencia, el informante puede elegir el cauce a seguir, interno o externo, según las circunstancias y los riesgos de represalias que considere.

En relación a las vías internas de comunicación se recomiendan las siguientes, a elección del informante:

- A través del formulario habilitado en el sitio web: <https://www.adara.vc/cumplimiento-normativo>
- A través de la plataforma interna [Canal de Denuncias](#)
- Mediante comunicación dirigida al Compliance Officer en C/José Abascal 58, 4D; 28003 Madrid

A solicitud del informante, canalizada por estos medios, también podrá presentarse mediante una reunión presencial dentro del plazo máximo de siete días.

Cualquier persona de la Sociedad que reciba una comunicación y no tenga competencias para investigar los hechos relatados deberá remitirla al Compliance Officer sin dilación indebida. La falta de observancia de esta obligación se considerará una infracción grave de las obligaciones de confidencialidad.

Los canales externos que en su caso el informante puede decidir utilizar se refieren a comunicaciones realizadas a las Instituciones, Organismos y Autoridades nacionales o europeas, a través de los medios determinados por éstas, y en particular a la Autoridad de Protección del Informante.

En determinados casos, y sólo para incumplimientos que produzcan efectos en el territorio de la comunidad autónoma, puede acudir a las Autoridades de Protección del Informante Autonómica, actualmente creada en: Cataluña, Valenciana, Illes Balears, Navarra, Principado de Asturias o Andalucía.

5. TRAMITACIÓN DE LAS COMUNICACIONES

Con carácter general el plazo máximo para dar respuesta a las actuaciones de investigación 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, éste podrá extenderse hasta un máximo de otros tres meses adicionales.

En las distintas fases del proceso de tramitación se prevé la posibilidad de mantener la comunicación con el informante y, si se considera necesario, de solicitar a la persona informante información adicional, salvo que haya renunciado a ello.

En todo caso se respetará el derecho a la presunción de inocencia y al honor de las personas afectadas, así como a las disposiciones sobre protección de datos personales de acuerdo a lo previsto.

Cuando los hechos pudieran ser indiciariamente constitutivos de delito la información se remitirá con carácter inmediato al Ministerio Fiscal. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

5.1 RECEPCIÓN Y REGISTRO DE LA COMUNICACIÓN

La información puede llevarse a cabo de forma anónima. En otro caso, se reservará la identidad del informante.

En los casos de comunicación verbal se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo con lo que establecen 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.

Al presentar la información, el informante podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones, pudiendo asimismo renunciar expresamente a la recepción de cualquier comunicación de actuaciones llevadas a cabo por la Sociedad como consecuencia de la información.

En caso de comunicación verbal, incluidas las realizadas a través de reunión presencial, el Responsable del sistema deberá documentarla 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.

Presentada la información, se procederá a su registro en el Sistema de Gestión de Información, siéndole asignado un código de identificación. El Sistema de Gestión de Información estará contenido en una base de datos segura y de acceso restringido, en la que se registrarán todas las comunicaciones recibidas, cumplimentando los siguientes datos:

- Fecha de recepción.
- Código de identificación.
- Actuaciones desarrolladas.
- Medidas adoptadas.
- Fecha de cierre.

Recibida la información, en un plazo no superior a 7 días naturales desde dicha recepción se procederá a acusar recibo de la misma, a menos que el informante expresamente haya renunciado a recibir comunicaciones relativas a la investigación, o salvo que ello pueda poner en peligro la confidencialidad de la comunicación.

5.2 TRÁMITE DE ADMISIÓN

Registrada la información, el Responsable del sistema comprobará si aquella expone hechos o conductas que se encuentran dentro del ámbito de aplicación del Anexo I, así como si resulta preciso reasignar la comunicación a otra persona o equipo gestor.

Realizado este análisis preliminar, decidirá, en un plazo que no podrá ser superior a diez días hábiles desde la fecha de entrada en el registro de la información:

- Inadmitir la comunicación cuando los hechos relatados carezcan de toda verosimilitud; no sean constitutivos de infracción; la comunicación carezca manifiestamente de fundamento; o no contenga información nueva y significativa sobre infracciones en comparación con una comunicación anterior.
- Admitir a trámite la comunicación. La admisión a trámite se comunicará al informante dentro de los siete días hábiles siguientes.
- Remitir con carácter inmediato la información al Ministerio Fiscal cuando los hechos pudieran ser indiciariamente constitutivos de delito.
- Remitir la comunicación a la autoridad, entidad u organismo que se considere competente para su tramitación.

5.3 INVESTIGACIÓN

La instrucción comprenderá todas aquellas actuaciones encaminadas a comprobar la verosimilitud de los hechos relatados.

Se garantizará que la persona afectada por la información tenga noticia de la misma, así como de los hechos relatados de manera sucinta. Adicionalmente se le informará del derecho que tiene a presentar alegaciones por escrito y del tratamiento de sus datos personales.

En ningún caso se comunicará a los sujetos afectados la identidad del informante ni se dará acceso a la comunicación. Durante la instrucción se dará noticia de la comunicación con sucinta relación de hechos al investigado.

Sin perjuicio del derecho a formular alegaciones por escrito, la instrucción comprenderá, siempre que sea posible, una entrevista con la persona afectada en la que, con absoluto respeto a la presunción de inocencia, se le invitará a exponer su versión de los hechos y a aportar aquellos medios de prueba que considere adecuados y pertinentes.

El Responsable del sistema estará obligado a guardar secreto sobre las informaciones que conozcan con ocasión de dicho ejercicio. Todas las personas de la Sociedad deberán colaborar con la investigación.

5.4 TERMINACIÓN DE LAS ACTUACIONES

Concluida la investigación el Responsable del sistema adoptará alguna de las siguientes decisiones:

- Archivo del expediente, que será notificado al informante y, en su caso, a la persona afectada.
- Remisión al Ministerio Fiscal si, pese a no apreciar inicialmente indicios de delito, así resultase del curso de la instrucción.
- Traslado de todo lo actuado a la autoridad competente.
- Adopción de acuerdo de inicio de un procedimiento sancionador.

Concluidas todas las actuaciones, el Responsable del sistema conservará información relacionada con la comunicación en un Libro Registro. Los datos personales relativos a las informaciones recibidas sólo se conservarán durante el período que sea necesario y proporcionado, y en ningún caso por un período superior a diez años.

Si en la resolución de la investigación se comprueba de forma fehaciente que los hechos investigados son ciertos y están vinculados a conductas irregulares o ilícitas, el denunciado podrá ser objeto de sanción de conformidad con el Convenio Colectivo Vigente de aplicación, la legislación laboral y el resto de las obligaciones civiles y mercantiles.

6. COMUNICACIÓN DE DENUNCIAS FALSAS O DE MALA FE

El canal de denuncias de la Sociedad debe emplearse de manera responsable y adecuada. La comunicación de hechos falsos, con una actitud maliciosa y moralmente deshonesto, supone una infracción de la buena fe que debe presidir las relaciones laborales y profesionales en la Sociedad, pudiendo derivar en medidas disciplinarias de conformidad con el Convenio Colectivo Vigente, o de tipo mercantil en el caso de otros stakeholders.

Si, tras el oportuno análisis, se pudiera concluir que los hechos denunciados son manifiestamente falsos y que la denuncia ha sido presentada con actitud maliciosa y mala fe: (i) se archivará la denuncia, (ii) se trasladará dicha circunstancia al Departamento de Personas para que se propongan medidas disciplinarias de conformidad con el Convenio Colectivo Vigente y; (iii) se informará, de forma escrita, la propuesta de sanción a la Dirección General de Personas o, en su caso, al Consejo de Administración, quien decidirá la acción disciplinaria a aplicar al denunciante de mala fe.

7. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Los tratamientos de datos personales que deriven de la aplicación del presente Procedimiento se registrarán por lo dispuesto en el artículo 11 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los Derechos Digitales, salvo que dicha comunicación tenga relación con cuestiones relativas a prevención del blanqueo de capitales y financiación del terrorismo y/o sanciones, en cuyo caso se aplicará lo dispuesto en la Ley 10/2010, de 28 de abril.

La Sociedad, como garantía de confidencialidad al informante, confirma que de forma general el ejercicio de los derechos de la persona investigada podría estar limitado por la particularidad de la comunicación y solo podrá ejercerse sobre los propios datos de carácter personal objeto de tratamiento. En ningún caso podrán entenderse incluidos dentro del ejercicio de los mencionados derechos por parte de la persona investigada los datos relativos al informante.

Responsable	Adara Ventures SGEIC SA
Finalidad	Gestionar, tramitar e investigar las comunicaciones remitidas a través del Canal de denuncias, así como para adoptar las medidas disciplinarias o tramitar los procedimientos que, en su caso, procedan.
Legitimación	Cumplimiento de una obligación legal
Destinatarios	Autoridades con competencia en la materia. Otras entidades de la Sociedad afectadas por la comunicación.
Derechos	Todos los derechos reconocidos en la normativa de protección de datos con las limitaciones establecidas en la Ley 2/2023 de protección del denunciante. Puede dirigirse a gdp@adara.vc para el ejercicio de sus Derechos.
Información ampliada	Puede ampliar información dirigiéndose a la política de Privacidad de la Sociedad: https://www.adara.vc/privacy-policy

8. LEGISLACIÓN VIGENTE

- 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
- Ley 10/2010, de 28 de abril de prevención de Blanqueo de Capitales
- Ley Orgánica 3/2018, de 5 de diciembre
- Ley 2/2023, de 20 de febrero de protección al denunciante
- Ley 35/2003, de 4 de noviembre, de Instituciones de Inversión Colectiva
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal
- Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Mercado de Valores
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 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

TIPOLOGÍA DE CASOS QUE SE PUEDEN REPORTAR A TRAVÉS DEL CANAL DE DENUNCIAS

Categoría	Subcategoría	Definición
Código general de Conducta	Comercialización de productos y servicios	Comercializar productos o servicios sin cumplir la obligación de tratar al cliente de forma justa actuando con honestidad, imparcialidad y profesionalidad.
	Conflictos de interés	Situaciones en las que los intereses personales o financieros de un empleado interfieran de alguna manera con su capacidad de servir a los mejores intereses de la Sociedad y sus stakeholders.
	Regalos e invitaciones	Cuando un profesional abusa de sus funciones ofreciendo, entregando, prometiendo, solicitando o aceptando cualquier tipo de regalo, beneficio o invitación para obtener una ventaja personal.
	Corrupción, soborno y cohecho	Un acto de corrupción puede surgir cuando un individuo abusa de su posición de poder o responsabilidad para su propio beneficio personal. El soborno son actos que dan a alguien la ventaja financiera o de otro tipo para animar a esa persona a desempeñar sus funciones de forma indebida.
	Prevención de Blanqueo de Capitales y Financiación del Terrorismo y Sanciones	El blanqueo de capitales incluye la conversión, ocultación, adquisición o posesión de bienes procedentes de actividades delictivas, así como la participación o tentativa de comisión de dichos actos.
	Privacidad/Seguridad de la Información/Confidencialidad	Abstenerse de difundir información a terceros: información personal de clientes, empleados, seguridad/estrategia de la Sociedad, así como información relativa a entidades con las que la Sociedad mantiene relaciones comerciales.
	Fraude Interno	Fraude intentado o perpetrado por una o varias partes internas contra la organización, incluidos los casos en que un empleado actúa en colusión con partes externas.
	Ciberseguridad	Acceso no autorizado o uso indebido de información o sistemas; fraude financiero y robo; alteración de la actividad comercial (sabotaje, extorsión, denegación de servicio).
	Igualdad de oportunidades y no discriminación	Conductas no alineadas con el principio de proporcionar las mismas oportunidades en el acceso al trabajo y en la promoción profesional, asegurando la ausencia de discriminación por razón de sexo, raza, religión, discapacidad, origen, estado civil, edad o condición social.
	Acoso Sexual o por Razón de Sexo	Comportamiento irrespetuoso o conducta no deseada de carácter sexual que genere un ambiente intimidatorio, ofensivo u hostil en el trabajo.
	Acoso laboral	Trato hostil o vejatorio de manera sistemática en el ámbito laboral que provoca un ambiente intimidatorio, ofensivo u hostil.
Contabilidad y Auditoría	Contabilidad y auditoría	Alteración o falsificación de la información financiera, inexactitudes en declaraciones financieras, falsedad intencionada en información, influencia indebida sobre los auditores.
Cuestiones laborales e incumplimiento de normativa interna	Incumplimiento de comportamientos corporativos	Conducta no profesional por parte de compañeros de trabajo o directivos no alineada con los comportamientos corporativos de la Sociedad.

	Faltas de respeto graves	Conductas que involucren faltas de respeto graves por parte de compañeros de trabajo o directivos en el entorno laboral.
	Incumplimiento de normativa interna o laboral	Todo incumplimiento de los reglamentos, políticas o procedimientos internos de la Sociedad que implique el incumplimiento de una obligación laboral.