AMICORP CAPITAL MANAGEMENT, SGEIC, S.A.U.

POLÍTICA DEL SISTEMA INTERNO DE INFORMACIÓN Y DE PROTECCIÓN AL INFORMANTE

Índice

1. Objeto

El objeto de la presente política es establecer los principios generales del Sistema Interno de Información de conformidad con lo establecido 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 ("**Ley 2/2023**"), que transpone al ordenamiento jurídico español la Directiva (UE) 2019/1937 del Parlamento 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, conocida como Whistleblowing Directive (la "**Política**").

El Sistema Interno de Información de Amicorp Capital Management, SGEIC, S.A. ("**Amicorp**" o la "**Entidad**") se trata de una herramienta a disposición de sus empleados, altos directivos, miembros del órgano de administración, accionistas y cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores, de acuerdo con el ámbito de aplicación subjetivo de la presente Política, con la finalidad de poder recibir de forma confidencial o anónima cualquier posible irregularidad o acto que se sospeche o conozca que son indebidos o contrarios a la legislación vigente o la normativa interna de la Entidad (en adelante, **el** "**Sistema Interno de Información**").

2. Ámbito de aplicación

2.1. Ámbito de aplicación subjetivo

La presente Política es de aplicación y obligado cumplimiento para todas las personas empleadas, integrantes del órgano de gobierno y la alta dirección de Amicorp y a aquellas personas que presten sus servicios de manera habitual sin formar parte de la plantilla, así como las personas que tengan la condición de trabajadores por cuenta ajena de la Entidad, accionistas y partícipes de la misma.

Asimismo, la presente Política se aplica a cualquier persona, física o jurídica, con quienes la Entidad tiene, o prevé establecer, algún tipo de relación de negocios, como proveedores o empleados de las entidades en las que se haya externalizado alguna de las funciones de la Entidad.

Además de los anteriores sujetos, podrán utilizar el Sistema Interno de Información personas con condición de empleados públicos, autónomos o trabajadores por cuenta ajena, así como todas aquellas personas que hayan tenido una relación laboral o estatutaria ya finalizada, voluntarios, becarios, trabajadores en periodos de formación con independencia de que perciban o no una remuneración, así como a aquellos cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.

Las diferentes medidas de protección previstas a lo largo de la presente Política se ejercerán según correspondan sobre todas las personas Informantes, los terceros relacionados y las personas afectadas por la comunicación recibida a través del Sistema.

Se entiende por "**Informante**" toda aquella persona que presente mediante el Sistema Interno de Información una comunicación relativa a las conductas listadas en el ámbito de aplicación objetivo que se describe a continuación.

Se entiende por los "**terceros relacionados**" aquellas personas que, en el marco de la organización en la que preste servicios el Informante, asistan al mismo en el proceso, así como que estén relacionadas con el Informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del Informante, y personas jurídicas, para las que trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa.

Se entiende por "**personas afectadas por la comunicación**" aquellas personas a las que se les atribuya mediante una comunicación presentada a través de los canales que integran el Sistema Interno de Información algunas de las conductas listadas en el ámbito de aplicación objetivo.

2.2. Ámbito de aplicación objetivo

A través de los diferentes canales que se integran en el Sistema Interno de Información, los Informantes podrán comunicar el conocimiento o sospecha motivada de conductas irregulares en:

a) Las infracciones del Derecho de la Unión Europea siempre que entren dentro del ámbito de aplicación de los actos de la UE enumerados en el anexo de la Directiva 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019 y que afecten a los intereses financieros de la UE o incidan en el mercado interior.

b) Infracciones de Derecho Laboral en materia de seguridad y salud en el trabajo.

c) Infracciones penales o administrativas graves o muy graves.

d) Infracciones del Reglamento Interno de Conducta de la Entidad, del Manual de Prevención de Blanqueo de Capitales y de la Financiación del Terrorismo o de cualquier otra Política de las desarrolladas y aprobadas conforme al Sistema de Gestión de Cumplimiento en la Entidad.

Asimismo, Amicorp como gestora de vehículos de inversión de tipo cerrado, y al tratarse de una entidad regulada, está sujeta a cierta normativa sectorial específica a la cual se debe prestar especial atención. Por tanto, a través del Sistema Interno de Información, se deberán informar, entre otras, sobre posibles infracciones de:

- *Ley 22/2014, de 12 de noviembre, por la que se regulan las entidades de capital-riesgo, otras entidades de inversión colectiva de tipo cerrado y las sociedades gestoras de entidades de inversión colectiva de tipo cerrado, y por la que se modifica la Ley 35/2003, de 4 de noviembre, de Instituciones de Inversión Colectiva* ("**Ley 22/2014**").
- En las cuestiones no regulada por la Ley 22/2014, la *Ley 35/2003, de 4 de noviembre, de Instituciones de Inversión Colectiva* ("**Ley 35/2003**").
- La *Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo* ("**Ley 10/2010**");

3. Responsable del Sistema Interno de Información

El responsable del Sistema Interno de Información desarrollará sus funciones de forma independiente y autónoma respecto del resto de los órganos de la Entidad, sin poder recibir instrucciones de ningún tipo en su ejercicio (el "**Responsable del Sistema**").

Se ha designado a la función de Cumplimiento Normativo como responsable de la gestión del Sistema Interno de Información, atendiendo al principio de proporcionalidad. Sin embargo, excepcionalmente, podrán acceder a la información contenida en las denuncias las personas con funciones de gestión y control en el área de Recurso Humanos en aquellos casos en los que sea necesario proceder a la adopción de medidas disciplinarias contra una persona. También tendrán acceso a cierta información las personas responsables de los servicios jurídicos, en aquellos casos en los que proceda la adopción de medidas legales en relación con los hechos relatados en las denuncias.

Por otro lado, la Entidad cuenta con un Delegado de Protección de Datos que podrá tener acceso a los datos personales contenidos en las denuncias en caso de que sea necesario para cualquier gestión relacionada con el tratamiento de dichos datos personales.

El Consejo de Administración designará, destituirá o cesará al Responsable del Sistema Interno de Información de conformidad con lo previsto en la Ley 2/2023. Tanto el nombramiento como el cese serán notificados a Oficina Antifrau de Catalunya en el plazo de diez días hábiles especificando, en el caso de su cese, las razones que han justificado el mismo, así como a la Autoridad Independiente de Protección al Informante (AIPI) en el plazo máximo de dos meses.

El Responsable del Sistema tramitará diligentemente el procedimiento de gestión de informaciones recopiladas mediante los canales que se integran en el Sistema Interno de Información (recogidos en el Apartado 5 de la presente Política) y aprobado por el Consejo de Administración. En el Procedimiento de gestión de informaciones del Sistema Interno de Información se establecerán las medidas para los supuestos de ausencia, enfermedad o vacancia o conflicto de interés del Responsable del Sistema.

4. Principios del Sistema Interno de Información

Los principios básicos sobre los que se fundamenta esta Política son los que se detallan a continuación:

a) **Independencia e imparcialidad**: El Responsable del Sistema deberá desarrollar sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad y ejercerá su labor de forma imparcial.

b) **Confidencialidad y anonimato**: Se garantizará el anonimato del Informante, si lo desea, y en todo caso la máxima confidencialidad de su identidad, de la información comunicada y de las actuaciones que se desarrollen siguiendo el Procedimiento de gestión de informaciones. Los datos derivados de las denuncias se tratarán de acuerdo a lo dispuesto en el *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 y por el que se deroga la Directiva 95/46/CE* ("**RGPD**") y la *Ley Orgánica 3/2018 de 5 de diciembre, de*

Protección de Datos Personales y garantía de los derechos digitales ("**Ley Orgánica 3/2018**").

c) **Respeto a los derechos fundamentales**: El Procedimiento de gestión de informaciones velará por todos los derechos fundamentales de las personas involucradas en el mismo, en especial por el derecho a la presunción de inocencia, el derecho al honor, el derecho de defensa, el derecho a la protección de datos, la intimidad y el secreto de las comunicaciones.

d) **Protección al Informante y 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 información a través del Sistema Interno de Información. Se entiende por represalia cualesquiera actos u omisiones que estén prohibidos por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional como consecuencia de la información presentada mediante el Sistema de Información Interno.

e) **Protección a las personas afectadas por la información**: Las personas afectadas por la información tendrán garantizado en todo momento su derecho a la presunción de inocencia, así como su derecho a una audiencia justa y demás derechos mencionados en el apartado c) del presente precepto.

f) **Transparencia**: La información sobre el Sistema Interno de Información estará publicada en la página web de la Entidad y en la intranet de la misma y se transmitirá de forma clara y comprensible.

g) **Celeridad y diligencia**: el Responsable del Sistema tramitará las informaciones recopiladas mediante los Sistemas Internos de información de conformidad con el Procedimiento de gestión aprobado el cual ha de garantizar que la investigación y resolución sobre los hechos se tramitan con la debida profesionalidad, diligencia y sin demoras indebidas.

h) **Buena fe**: Se velará por que la información comunicada sea honesta, íntegra y veraz. La Entidad no permitirá el uso de los Sistemas Internos de Información bajo móviles personales, ilegítimos o contrarios a la buena fe.

i) **Formación y difusión**: Informar a todos los empleados y directivos de Amicorp sobre la existencia de los canales disponibles, destacando su importancia para crear un ambiente laboral positivo. Para lograr lo anterior, se llevarán a cabo regularmente iniciativas de concienciación y formación donde se explicará la relevancia del Sistema Interno de Información, así como sus características y cómo utilizarlo.

j) **Deber de información**: Obligación de informar de comunicar cualquier presunta infracción penal o administrativa grave o muy grave, así como cualquier acto presuntamente ilícito, tanto para el personal de Amicorp como para los miembros de la alta dirección.

5. Canales que integran el Sistema Interno de Información

Los Informantes pueden hacer llegar el formulario incluido en el Anexo I de la presente Política facilitado para llevar a cabo las comunicaciones a través los siguientes canales:

- Por correo electrónico: canaldenuncias@amicorpcapitalmanagement.es
- Para aquellas personas que deseen hacer uso del carácter anónimo de su denuncia, por dirección postal:

- AMICORP CAPITAL MANAGEMENT, S.G.E.I.C., S.A.U.
- A la atención de: Cumplimiento Normativo
- C/ Pau Claris, nº 165, 3ª planta Puerta B
- Barcelona

6. Publicidad

La presente Política se entrega y está a disposición de todas las personas que forman parte de la Entidad, así como de los socios de negocio y terceras partes, mediante su publicación en la intranet del Grupo Amicorp y en la página web de la Entidad.

Igualmente, se realizará la comunicación oportuna de difusión y comunicación interna mediante las herramientas existentes, para su comprensión y aplicación.

7. Garantías para el Informante

7.1. Confidencialidad y anonimato

Se garantiza la confidencialidad en la tramitación de las comunicaciones a través del Sistema Interno de información y las correspondientes investigaciones internas en los términos previstos en la presente Política. En caso de que una comunicación se realice por una vía distinta del Sistema Interno de información ante cualquier profesional, directivo, consejero o empleado de la Entidad, el receptor de la comunicación también estará sujeto a la citada obligación de confidencialidad y deberá remitir la comunicación inmediatamente a través del Sistema Interno de información.

La garantía de confidencialidad de la identidad del Informante constituye uno de los principios rectores del funcionamiento del Sistema Interno de información, de modo que esta información no será revelada a ninguna persona distinta de aquellas que participen conforme a esta Política en la recepción y tramitación de la comunicación y, en su caso, de la correspondiente investigación interna e implementación de medidas correctoras, legales o disciplinarias que resulten pertinentes. En ningún caso se comunicará a la persona investigada o afectada por la comunicación la identidad del Informante ni ningún dato personal que directa o indirectamente permita su identificación.

Sin perjuicio de lo anterior, la identidad del Informante podrá comunicarse a la autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora, en los términos del artículo 33.3 de la Ley 2/2023. En estos casos, se trasladará al Informante esta necesidad de comunicación antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial.

El Sistema Interno de información admite la posibilidad de formular comunicaciones anónimas, debiendo la Entidad abstenerse de realizar cualquier acción tendente a revelar la identidad del Informante salvo que ello se derive del cumplimiento de una obligación legal o impuesta por la autoridad judicial o administrativa competente.

7.2. **Prohibición de represalias y medidas de protección a las personas afectadas**

Las personas que realicen comunicaciones de buena fe estarán protegidas frente a cualquier forma de discriminación, represalia o consecuencia negativa derivada de la denuncia. Asimismo, no se tolerará que otros adopten medidas adversas contra quienes informen de buena fe sobre conductas ilegales o poco éticas.

Quedan prohibidos expresamente los actos de represalia, incluidas las amenazas y tentativas de represalia, contra quienes presenten una comunicación conforme a la ley. Se considerará represalia cualquier acto u omisión ilícito o que, directa o indirectamente, suponga un trato desfavorable que coloque al Informante en una situación de desventaja en el ámbito laboral o profesional, por el hecho de informar o realizar una revelación pública.

A los efectos del artículo 36.3 de la Ley 2/2023, se consideran represalias:

a) Suspensión del contrato de trabajo, despido o extinción de la relación laboral o estatutaria, incluyendo la no renovación o la terminación anticipada de un contrato de trabajo temporal una vez superado el período de prueba, o terminación anticipada o anulación de contratos de bienes o servicios, imposición de cualquier medida disciplinaria, degradación o denegación de ascensos y cualquier otra modificación sustancial de las condiciones de trabajo y la no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido; salvo que estas medidas se llevaran a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral o reguladora del estatuto del empleado público correspondiente, por circunstancias, hechos o infracciones acreditadas, y ajenas a la presentación de la comunicación.
b) Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.
c) Evaluación o referencias negativas respecto al desempeño laboral o profesional.
d) Inclusión en listas negras o difusión de información en un determinado ámbito sectorial, que dificulten o impidan el acceso al empleo o la contratación de obras o servicios.
e) Denegación o anulación de una licencia o permiso.
f) Denegación de formación.
g) Discriminación, o trato desfavorable o injusto.

El Informante que entienda que se ha tomado alguna represalia en su contra como consecuencia de, exclusivamente, haber presentado una denuncia, podrá ponerlo en conocimiento del Responsable del Sistema Interno de información a través de cualquier medio de comunicación del Sistema Interno de Información, que estudiará el caso y tomará las medidas adecuadas para prevenirla o, en su defecto, corregirla.

El Informante que viera lesionados sus derechos por causa de su comunicación una vez transcurrido el plazo de dos (2) años, podrá solicitar la protección de la autoridad competente que, excepcionalmente y de forma justificada, podrá extender el periodo de protección, previa audiencia de las personas u órganos que pudieran verse afectados.

La prohibición de represalias prevista en este apartado no impedirá la adopción de las medidas disciplinarias que procedan cuando la investigación interna determine que la comunicación es falsa y haya sido formulada con mala fe por parte del Informante o se haya determinado que el Informante incumplió los comportamientos corporativos o actuara de manera ilegal.

Las personas que comuniquen alguna información a través del Sistema Interno de Información gozarán de la protección frente a represalias, siempre y cuando la comunicación se haya realizado de buena fe y conforme a los requerimientos previstos en esta Política y demás normativa aplicable. Quedarán excluidas de esta protección las personas que:

a) Presenten una comunicación con informaciones contenidas en comunicaciones previas que hayan sido previamente inadmitidas por alguna de las causas previstas en esta Política.
b) Informen de conflictos interpersonales que afecten únicamente al Informante y a las personas a las que se refiera la comunicación.
c) Comuniquen informaciones públicas o que constituyan meros rumores.
d) Comuniquen informaciones que se refieran a acciones u omisiones no comprendidas en el ámbito de aplicación del Sistema Interno de Información, de acuerdo con esta Política.

La prohibición de represalias prevista en los párrafos anteriores no impedirá la adopción de las medidas disciplinarias que procedan cuando la investigación interna determine que la denuncia es falsa y que la persona que la ha realizado era consciente de su falsedad, habiendo actuado así con mala fe.

8. Tratamiento de datos de carácter personal

8.1. Identidad del responsable del tratamiento

Los datos personales que pueden llegar a tratarse en el curso de una investigación dentro del Procedimiento de gestión del Sistema Interno de Información son responsabilidad de AMICORP CAPITAL MANAGEMENT, SGEIC, S.A., con NIF A-75990119, con domicilio social en Pau Claris, 165 - 08037 Barcelona (Barcelona).

8.2. Delegado de Protección de Datos

Amicorp cuenta con un Delegado de Protección de Datos que se encarga de supervisar el cumplimiento de protección de datos, con quien se podrá contactar a través de la dirección electrónica:

privacy@amicorp.com

8.3. Tratamiento de datos personales

En el marco del proceso de tramitación e investigación de las denuncias, Amicorp recabará los siguientes datos personales:

- Nombre y datos de contacto del Informante, en caso de que se trate de una denuncia no anónima. El Informante puede también identificarse voluntariamente en un momento posterior a la interposición de la denuncia o aportar en un momento posterior del proceso documentación o información adicional.

- Información facilitada tanto en el momento de la denuncia como durante toda la tramitación del expediente. Esta información contendrá una descripción precisa y circunstanciada de los hechos denunciados, la fecha aproximada de la acción irregular, el área afectada y su posible impacto, así como evidencias precisas que soporten la denuncia.
- Nombre y otros datos personales de las personas que menciona la denuncia (supuesto infractor, posibles testigos y otros), si proporciona dicha información (es decir, descripción de las funciones y datos de contacto y participación o rol respecto a los hechos denunciados).

Dependiendo de los hechos que se denuncien, Amicorp podrá llegar a acceder a:

(i) Toda la información facilitada por parte del Informante (incluso de entrevistas si fuera necesario);

(ii) Información facilitada por terceros como: testigos, familiares, el denunciado, peritos, fuerzas y cuerpos de seguridad del Estado, terceros externos como investigadores o consultores especializados;

(iii) Todos los documentos facilitados o relacionados con el hecho denunciado; y

(iv) A los recursos de tecnologías de la información asignados al Informante y denunciado, incluyendo, con carácter no limitativo, su correo corporativo, así como cualesquiera otros recursos informáticos suministrados por Amicorp.

En todo momento, sólo se tratarán los datos personales que sean estrictamente necesarios para los fines de gestionar, tramitar e investigar las denuncias relativas a la comisión de irregularidades, a fin de llevar a cabo las actuaciones necesarias para la investigación de los hechos denunciados, incluidas, en su caso, adopción de las medidas disciplinarias o legales que correspondan.

8.4. **Finalidad del tratamiento**

La finalidad del tratamiento de datos personales del Sistema Interno de Información es la de gestionar la comunicación de una conducta irregular a través de este canal cuando el Informante haya informado sobre sospechas de conductas irregulares, actos ilícitos o incumplimientos normativos. Amicorp pondrá a disposición de los usuarios que sean empleados, proveedores o cualquier tercero con interés legítimo la posibilidad de denunciar a través del Sistema Interno de Información cualquier conducta que pudiera resultar irregular, así como cualesquiera actos ilícitos o incumplimientos normativos.

Los datos personales no serán utilizados para una finalidad distinta de la indicada.

8.5. **Legitimación del tratamiento**

El tratamiento de los datos personales que se realice en el marco de la gestión e investigación de denuncias recibidas se realiza sobre la base del artículo 6.1.c) del RGPD (en cumplimiento de una obligación legal) o en virtud del artículo 6.1.e) del RGPD (en cumplimiento del interés público). Adicionalmente, el tratamiento de categorías especiales de datos que se produzca en el marco del Sistema Interno de Información queda amparado por la excepción del artículo 9.2.g) del RGPD (razones de interés público esencial).

La normativa aplicable en España establece la obligatoriedad de establecer canales de comunicación y reconocen en estos una excelente herramienta para la prevención de delitos de forma eficaz, incluyendo como destinatarios a la totalidad de sujetos de la empresa (empleados,

directivos, etc.) como parte del control interno de esta en materia de gestión de riesgos. En particular:

- La propia Ley 2/2023

- El Código Penal, que establece en su artículo 31 bis 2. 4º la "obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y la observancia del modelo de prevención". De manera implícita, las empresas deben proporcionar un canal a través del cual se pueda enviar la información.

- La Ley 10/2010, que establece en su artículo 26.bis la obligación de los sujetos obligados a establecer procedimientos para que sus empleados, directivos o agentes puedan comunicar, incluso anónimamente, información relevante sobre posibles incumplimientos de esa ley, su normativa de desarrollo o las políticas y procedimientos implantados.

8.6. **Derecho de información**

El Responsable del Sistema Interno de Información deberá informar a la persona acusada en la denuncia interpuesta de las acciones u omisiones que se le atribuyen. Esta comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.

Durante la tramitación del expediente las personas objeto de la denuncia tendrán el derecho a ser consideradas inocentes hasta que se demuestre lo contrario, así como el derecho a la defensa y acceder a la documentación del expediente. Estos derechos serán equiparados a los otorgados a los Informantes, preservando la identidad de estos últimos y garantizando la confidencialidad de los hechos y datos relacionados con el procedimiento.

En particular, se informará a la persona investigada, al menos, de lo siguiente:

a) la persona o personas encargadas de la investigación;

b) los hechos de los que se le acusa;

c) los departamentos y servicios afectados y que podrían conocer el asunto dentro de Amicorp en función de la evolución de la investigación;

d) del tratamiento que se va a dar a sus datos de conformidad con el artículo 14 del RGPD, con identificación del responsable de dicho tratamiento, la fuente de obtención de la información, la tipología de datos tratados y la finalidad y legitimación del tratamiento (en este caso la propia investigación) y la adopción de las medidas que sean necesarias, así como del periodo de conservación de la información y posibles comunicaciones a terceros;

e) sus derechos en materia de protección de datos (acceso, rectificación, supresión y oposición, limitación del tratamiento y portabilidad);

f) la posibilidad que tiene de solicitar ser asistido por un abogado durante el proceso de investigación interna; y

g) la posibilidad de acudir a canales externos de comunicación de denuncias ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la UE.

El momento en el que se informe a la persona investigada variará según las circunstancias de cada caso. Se procurará informar a la persona investigada tan pronto como sea posible, pero siempre persiguiendo el objetivo de conservar las pruebas evitando su alteración o destrucción por parte del denunciado.

En los casos en los que el Responsable del Sistema Interno de Información considere que existe el riesgo de que la persona investigada pueda alterar o destruir pruebas relacionadas con los hechos denunciados, o bien la información al Informante pueda suponer una obstaculización de los logros de la eventual investigación, de conformidad con las excepciones del artículo 14.5 RGPD, y siempre a criterio del Responsable del Sistema Interno de Información, podrán evitar comunicar dicha información al Informante hasta el momento del trámite de audiencia.

8.7. **Conservación de los registros**

Los datos personales que se recaben serán conservados:

(i) durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados;

(ii) durante el tiempo en que se desarrollen las actuaciones de investigación y, finalmente,

(iii) a lo largo del ejercicio de las acciones legales que correspondan.

Todas las denuncias y consultas que se reciban por el Sistema Interno de Información, las contestaciones que se den a la persona denunciante, toda la documentación que se genere en la investigación, entrevistas, etc. serán conservados en el libro-registro de Amicorp. 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 y durante un plazo máximo de diez (10) años.

Los datos que sean objeto de tratamiento podrán conservarse en el Sistema Interno de Información únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

En todo caso, transcurridos tres (3) 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 establecida en el artículo 32 de la Ley Orgánica 3/2018.

Una vez transcurrido el plazo mencionado en el párrafo anterior, los datos podrán seguir siendo tratados por el órgano al que corresponda para la investigación de los hechos denunciados, no conservándose en el propio Sistema Interno de Información. Asimismo, los datos personales se podrán conservar para:

(i) dar cumplimiento a posibles obligaciones legales que resulten de aplicación, así como

(ii) atender a posibles reclamaciones y responsabilidades.

8.8. **Destinatario de los Datos**

Como regla general, no se cederán a ningún tercero los datos que se recaben a través del Sistema Interno de Información. Asimismo, únicamente podrá acceder a ellos el personal que, por sus funciones, responsabilidades y cometidos, esté debida y previamente autorizado.

No obstante, la información recabada a través del Sistema Interno de Información se podrá facilitar a los organismos públicos competentes, por ejemplo, Juzgados y Tribunales, Cuerpos y Fuerzas de Seguridad o cualquier otro competente, previo requerimiento por su parte, cuando la Entidad esté legalmente obligada.

8.9. **Derechos en materia de protección de datos**

Los usuarios del Sistema Interno de Información pueden ejercitar sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad, respecto del tratamiento del que es responsable Amicorp mediante escrito dirigido a Amicorp a la siguiente dirección electrónica: privacy@amicorp.com

Asimismo, en el caso que se entiendan vulnerados los derechos de protección de datos, se podrá presentar cualquier reclamación ante el Delegado de Protección de Datos de Amicorp o bien ante la Agencia Española de Protección de Datos, AEPD, www.aepd.es.

9. Aprobación y entrada en vigor

La presente Política será aprobada por el Consejo de Administración de la Entidad, así como las posteriores modificaciones que se produzcan.

Esta Política será objeto de revisión y actualización cuando sea necesario, al menos, en los siguientes casos:

- Cuando tengan lugar cambios legales o normativos que afecten a la Política o establecido.
- A propuesta de la Unidad de Cumplimiento Normativo cuando entienda que existan aspectos susceptibles de mejora para la consecución de los objetivos propuestos o para adaptarse convenientemente a las características de los servicios ofrecidos por la Entidad en cada momento. Como mínimo, se adoptarán medidas adicionales o alternativas cuando la Entidad acepte o autorice la utilización de un nuevo medio de comunicación.
- A propuesta de los órganos supervisores.

10. Cuadro de versiones

VERSIÓN	FECHA DE APROBACIÓN POR EL CONSEJO DE ADMINISTRACIÓN	CAUSAS DEL CAMBIO	MODIFICACION EFECTUADA
1.0	23 / 12/ 2025	Primera versión de la Política	N/A

Anexo I - Comunicación al responsable del sistema interno de información

☐ Denuncia anónima ☐ Comunicación no anónima (por favor, rellene los datos que se muestran a continuación): - Nombre y apellidos: - DNI: - Datos de contacto:
Finalidad
Asunto
Descripción de los hechos y fechas aproximadas de los hechos
Evidencias:

Si lo desea, indique un domicilio, o correo electrónico seguro a efectos de recibir notificaciones sobre el Procedimiento de gestión de comunicaciones:

_____

La estructura del presente formulario es orientativa. El Informante tiene potestad para usar o no el presente formulario de comunicación para hacer llegar la información mediante los canales establecidos.