Suma Capital
GROWING TOGETHER

SUMA CAPITAL, S.G.E.I.C, S.A., Sociedad Unipersonal

PROTOCOLO DEL SISTEMA INTERNO DE INFORMACIÓN

Versión	Fecha	Afecta	Breve descripción del cambio
1ª	22-05-2020	Creación	
2ª	15-05-2023	Actualización	Adaptación a 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 por la que se transpone la Directiva (UE) 2019/1937 del Parlamento Europeo.
3ª	24-05-2024	Actualización	Incorporación de Net Zero Ventures, S.L.
4ª	04-11-2024	Actualización	Inclusión expresa de canales externos de información y precisiones en materia de protección de datos.
5ª	23-10-2025	Actualización	Revisión de erratas y aclaraciones menores, sin cambios de fondo.

ÍNDICE

1. INTRODUCCIÓN 4
2. IDENTIFICACIÓN 5
2.1. OBJETO 5
2.2. ÁMBITO DE APLICACIÓN 6
3. DEFINICIONES 6
4. SISTEMA INTERNO DE INFORMACIÓN 7
4.1. COMUNICACIÓN DE UNA INFRACCIÓN 7
4.2. CONTENIDO DE LA COMUNICACIÓN DE INFRACCIÓN 9
4.3. PROCEDIMIENTO 10
5. CANAL EXTERNO DE INFORMACIÓN 14
6. DERECHOS, PRINCIPIOS Y GARANTÍAS 14
6.1. DERECHOS DEL INFORMANTE 14
6.2. PRINCIPIOS Y GARANTÍAS 15
6.3. CONFLICTO DE INTERESES 17
6.4. DERECHOS DE LAS PERSONAS INVESTIGADAS 18
7. INFORME Y REGISTRO DE LA COMUNICACIÓN DE INFORMACIONES TRAMITADAS 19
8. TRATAMIENTO DE DATOS PERSONALES 19

1. INTRODUCCIÓN

De conformidad con las exigencias recogidas 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 por la que se transpone la Directiva (UE) 2019/1937 del Parlamento Europeo (en adelante "Ley 2/2023") y en el Código Penal, art.31bis, **SUMA CAPITAL, S.G.E.I.C, S.A., Sociedad Unipersonal, y Net Zero Ventures, S.L.** (en adelante, "NZV"), sociedad asesora de algunos de los fondos gestionados por SUMA CAPITAL S.G.E.I.C., S.A., Sociedad Unipersonal (en adelante, conjuntamente, "**SUMA CAPITAL**") han procedido a la creación de un Sistema Interno de Información.

La Ley 2/2023, en su artículo 10.1.b), establece que las empresas del sector privado incluidas en el ámbito de aplicación de los actos de la Unión Europea relativos a los servicios, productos y mercados financieros, deberán contar con un Sistema Interno de Información, que se regirá por su normativa específica, con independencia del número de trabajadores de la entidad. Asimismo, el Código Penal, en el marco de la implementación del Modelo de Prevención de delitos, en su art.31.bis.5. 4º, requiere que se imponga la obligación en las empresas de informar de riesgos e incumplimientos del Modelo de Prevención de Delitos (en lo sucesivo "MPD") a los Compliance Officers.

Por lo anterior, y dado que la entidad tiene como principal interés la creación de una cultura empresarial de cumplimiento a la legalidad, es por lo que se ha creado el Sistema Interno de Información y se desarrolla el presente Protocolo.

2. IDENTIFICACIÓN

2.1. OBJETO

El presente documento tiene como objeto establecer el contenido de la **Política del Sistema Interno de Información (SII)**, en virtud de lo dispuesto en el artículo 5.2.h) de la Ley 2/2023, definiendo los principios generales que regulan los sistemas internos de información y la protección de los informantes, así como garantizando su difusión y conocimiento interno.

Asimismo, establece de manera clara el **procedimiento de tramitación de las comunicaciones de infracciones**, incluyendo las pautas de actuación que deben seguirse desde la recepción de la comunicación por parte de la **Compliance Officer** o del **Gestor Externo**, hasta la resolución final, asegurando su adecuada recepción, seguimiento, investigación y resolución.

El Sistema Interno de Información se configura como uno de los controles claves establecidos en el MPD para la prevención, detección y conocimiento de quebrantos éticos, incumplimientos normativos o ilícitos penales, de forma que las pautas que se recogen en este Protocolo son de obligado cumplimiento para todas las personas relacionadas con la entidad.

La entidad otorgará todos los recursos necesarios a la Compliance Officer para tramitar y resolver adecuadamente las comunicaciones de Infracciones que lleguen a través del Sistema Interno de Información, dotándoles, además, de autoridad, autonomía y acceso suficiente a la información de la entidad para que cumpla con sus funciones. Asimismo, SUMA CAPITAL garantiza una protección efectiva de los informantes frente a posibles represalias, promueve una cultura ética entre las personas trabajadoras y otros interesados, y fomenta la utilización del Sistema Interno de Información como mecanismo para la prevención y detección de riesgos y amenazas al interés público.

2.2. ÁMBITO DE APLICACIÓN

Este Protocolo es de aplicación y obligado cumplimiento por parte de todos los miembros de la entidad. Se incluye dentro del concepto "miembro":

- Empleados de la entidad.
- Los accionistas, partícipes o personas pertenecientes al Órgano de Administración.
- Profesionales y colaboradores vinculados a la entidad respecto a los que este pueda ostentar, directa o indirectamente, el control.
- Personal en prácticas.

3. DEFINICIONES

3.1. Sistema Interno de Información: Canal para comunicar **acciones u omisiones que constituyan infracciones**, gestionadas de manera efectiva y sin riesgo de represalia, incluyendo las **infracciones del Derecho de la UE** que cumplan las condiciones del **artículo 2 de la Ley 2/2023**.

3.2. Canal Externo de Información de la Autoridad Independiente de Protección del Informante: Sistema de información gestionado por parte de una autoridad estatal, así como autoridades autonómicas al que pueden acudir los empleados de la entidad.

3.3. Infracciones:

- Incumplimiento de normativa interna.
- Infracción penal o administrativa.
- Cualquier vulneración de la normativa estatal o de la Unión Europea.

3.4. Informante: Persona que comunica una infracción.

3.5. Persona investigada: Persona respecto a la que se interpone la comunicación de infracción y que como consecuencia de la investigación pude ser sancionada disciplinariamente o se le pueda

atribuir responsabilidad penal o administrativa.

3.6. Persona afectada: Persona que sufre los actos de la persona investigada diferente al Informante (en su caso).

3.7. Responsable del Sistema: Persona responsable del Sistema Interno de Información nombrada por el Órgano de Administración y encargada de gestionar y tramitar expedientes de investigación. En este caso, el Responsable del sistema será la Compliance Officer de la entidad.

3.8. Responsable de la investigación: persona designada por el Comité de Cumplimiento para llevar a cabo la investigación de una comunicación de infracción.

3.9. Gestor externo: Abogados externos que gestionan el Sistema Interno de Información.

3.10. Autoridad independiente de Protección del Informante (A.A.I): Autoridad estatal y autoridades autonómicas encargada de gestionar el sistema externo de información y de tramitar las denuncias interpuestas en dicho sistema.

4. SISTEMA INTERNO DE INFORMACIÓN

4.1. COMUNICACIÓN DE UNA INFRACCIÓN

La comunicación de Infracciones puede realizarse de forma escrita o de forma verbal. Independientemente de la vía de comunicación utilizada, en el caso de que pueda producirse algún conflicto de intereses en el tratamiento de dichas comunicaciones, o por alguna circunstancia se considere preferible una gestión externa, las mismas serán gestionadas por el Gestor Externo del Sistema, ASESORIA PENAL CORPORATIVA (en adelante, "APC").

4.1.1. Comunicación de Infracciones de forma escrita:

4.1.1.1. **Plataforma online:** Se ha habilitado un sistema interno

de información en la plataforma FACTORIAL a la que pueden acceder todos los empleados de SUMA CAPITAL, S.G.E.I.C., S.A, Sociedad Unipersonal, para la comunicación de Infracciones de forma segura y confidencial y que constituirá la vía preferente para la realización de comunicaciones. Los empleados de NZV tendrán disponible esta vía de comunicación a través del siguiente link, que asimismo se encuentra disponible en la página web de SUMA CAPITAL, S.G.E.I.C., S.A, Sociedad Unipersonal: Suma Capital - Canal seguro

A través de la plataforma, los miembros de la entidad pueden acceder a un formulario mediante el cual se puede interponer una comunicación de información nominativa o anónima. Estas informaciones serán gestionadas por la Responsable del Sistema Interno de Información.

Tras la interposición de la comunicación de información, el informante podrá acceder a la plataforma cuando lo estime oportuno en aras de conocer el estado de tramitación de la comunicación de infracción realizada.

4.1.1.2. Correo electrónico: alternativamente, el informante puede enviar un correo electrónico a la Compliance Officer, Responsable del Sistema Interno de Información: Dña. GRISELDA GARDE (ggarde@sumacapital.com) o al Gestor Externo APC (proyectos@asesoriapenalcorporativa.es) para comunicar una infracción.

4.1.1.3 Correo postal: alternativamente, el informante puede realizar la información por escrito a través de correo postal a la atención de la Compliance Officer al domicilio social de la entidad[1].

4.1.2. Comunicación de infracción de forma verbal:

4.1.2.1. En reunión presencial: a solicitud del informante (en los datos indicados con anterioridad), la información podrá presentarse mediante

[1] Av. Diagonal, nº. 640, (08017), Barcelona. CIF: A64096563

reunión presencial o telemática con la Compliance Officer y/o el Gestor Externo dentro del plazo de siete días desde la solicitud de la misma. La información mediante reunión presencial o telemática deberá ser grabada. En este sentido, los Compliance Officer y/o el Gestor Externo deberán advertir de este aspecto al informante y se le informará del tratamiento de sus datos de acuerdo a los establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

4.1.2.3 Información comunicada por otros medios: en el supuesto de que una información sea remitida por otros medios o canales no establecidos en este protocolo, o bien a miembros de la entidad no responsables de su tratamiento, deberán ser comunicadas por el receptor mediante el sistema interno de información de la entidad.

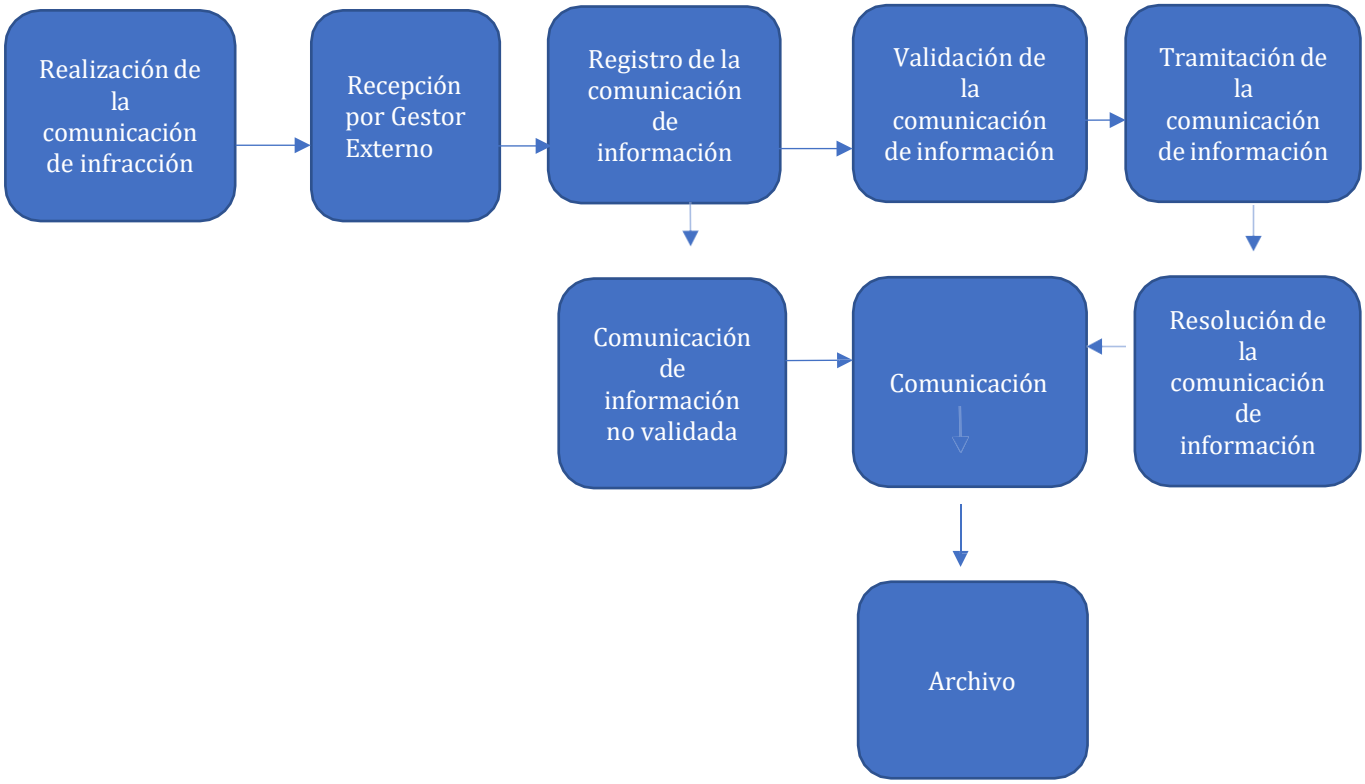
4.2. CONTENIDO DE LA COMUNICACIÓN DE INFRACCIÓN

El contenido de la comunicación de infracción debe ser el siguiente:

- Identificación del informante (nombre completo, DNI, correo electrónico y vinculación con la entidad) o marcar la opción anónimo.
- Identificación del departamento y/o actividad dónde se han producido los hechos o dónde se ha tenido conocimiento de los indicios referenciados.
- Nombre de la persona/s investigada o delimitación del área (si se conoce).
- Descripción de los hechos y circunstancias en las que ocurrieron.
- Todos los medios de prueba al alcance del informante que sean relevantes, oportunos y lícitos.
- Fecha en la que se produjeron los hechos.
- Personas que han presenciado o tienen conocimiento de los hechos.
- Cómo se ha tenido conocimiento del hecho comunicado.

Toda comunicación de información deberá ser interpuesta de buena fe.

4.3. **PROCEDIMIENTO**



4.3.1. **Recepción de la comunicación de infracción**: APC, como Gestor Externo y la Compliance Officer, como Responsable del Sistema Interno de Información recibirán la comunicación de infracción a través de la plataforma o los medios alternativos referidos anteriormente y se registrarán las actuaciones que se lleven a cabo.

La Compliance Officer o, en caso de ser necesario, APC dispondrán del plazo de 7 días naturales siguientes a su recepción para remitir un acuse de recibo al informante, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.

4.3.2. **Registro de la comunicación de infracción:** Una vez interpuesta la comunicación a través de la plataforma, la misma quedará registrada

de forma automática en la misma. En el caso de que la información se interponga por otro medio, como la reunión presencial, se deberá llevar a cabo el registro pertinente de dicha información por parte de la Compliance Officer y/o el Gestor Externo.

4.3.3. **Comunicación de infracción válida:** En el caso de que la comunicación de la Infracción se refiera a incumplimientos que se enmarcan en el ámbito objetivo del Canal (Infracciones indicadas en el punto 3.3) la comunicación de Infracción será validada.

4.3.4. **Comunicación de información no válida:** en el caso de que la comunicación de información se refiera a hechos que

- quedan fuera del ámbito objetivo de aplicación del canal (punto 3.3.) o que carezcan manifiestamente de fundamento: será comunicado al informante y se procederá al archivo de la comunicación de información,
- sean ajenos al ámbito objetivo del canal, pero relevantes para la entidad: serán remitidas al departamento correspondiente para el tratamiento de la incidencia, será comunicado al informante y se procederá al archivo de la comunicación de información.

4.3.5. **Tramitación de la comunicación de infracción:** la comunicación de infracción que haya sido previamente validada será tramitada. Ello significa que se dará inicio a la investigación interna pertinente. En este sentido, la Compliance Officer, como Responsable del Sistema Interno de Información, si lo considera necesario, nombrará a un Responsable de la Investigación. En el caso de que la información haya sido gestionada por el Gestor Externo, la misma será compartida con la Comité de Cumplimiento, respetando las normas de conflicto de intereses del apartado 5.3 del presente protocolo. En su caso, el receptor de la información podrá nombrar a un Responsable de la Investigación.

En este sentido, la investigación interna podrá ser llevada a cabo por:

- uno o varios miembros del Comité de Cumplimiento no afectados por la información.
- un miembro de la entidad que se considere competente en caso de que la información afecte directamente a todos los miembros del Comité de Cumplimiento.
- un experto o asesor externo.
- un órgano compuesto por varias personas de la entidad con o sin un experto o asesor externo siempre que respecto a los mismos no exista incompatibilidad o un conflicto de intereses.

El Responsable de la Investigación llevará a cabo las actuaciones que considere necesarias de forma individual o en colaboración con las personas que considere necesario, siempre que sobre las mismas no exista incompatibilidad o conflicto de interés. Para ello podrá recabar toda la información y documentación que considere necesaria de cualquier área, división o departamento, respetando siempre los derechos fundamentales de la/s persona/s que sean objeto de investigación. En caso de que se considere necesario, se podrá contar como complemento necesario e indispensable para salvaguardar la garantía de independencia con un asesor experto externo para la investigación y realización del dictamen.

En este sentido, durante la investigación, el responsable de la misma podrá mantener comunicación con el informante y, si lo considera necesario, solicitarle información adicional.

La duración máxima de las actuaciones de investigación será de tres meses desde la recepción de la comunicación de infracción hasta la resolución de la misma o, si no se remitió acuse de recibo al informante, desde la finalización del plazo de siete días después de la comunicación. En casos de especial complejidad, que

deberán justificarse por escrito por parte del Responsable de la Investigación, podrá ampliarse el plazo por tres meses adicionales.

4.3.6. **Resolución de la comunicación de infracción:** Concluida la investigación, el Responsable de la Investigación realizará un informe que compartirá con la Compliance Officer y con los miembros del Comité de Cumplimiento para su aprobación y posterior reporte al Órgano de Administración.

4.3.7. **Comunicación al Informante:** aprobado el Informe, se comunicará al Informante que la tramitación de la comunicación de información ha concluido y que se procederá al archivo de la misma.

4.3.8. **Archivo**: tras la comunicación al Informante, la comunicación de información será archivada.

Del todo el procedimiento constará un reflejo en la plataforma online a la que tendrá acceso el Informante que haya interpuesto una comunicación de información para poder consultar el estado de la tramitación de la misma (no su contenido). En el caso de que la comunicación de información se haya interpuesto por email, teléfono o de forma presencial, las comunicaciones se realizarán por correo electrónico.

Lo anterior sucederá salvo en los casos en que el Informante indique que no quiere recibir información del procedimiento, supuestos en los que no se le remitirá comunicación alguna.

En los reportes que se realicen al Órgano de Administración se incluirá información relativa a la comunicación de información tramitada omitiendo aquella información que permita la identificación del informante, es decir se anonimizará la información en el reporte.

5. CANAL EXTERNO DE INFORMACIÓN

Toda persona podrá informar sobre la comisión de cualquier acción u omisión incluida en el ámbito de aplicación del presente Protocolo ante la **Autoridad Independiente de Protección del Informante (A.I.P.I.)** o ante las autoridades u órganos autonómicos correspondientes.

Esta comunicación puede realizarse de manera directa o previa comunicación a través del Sistema Interno de Información habilitado por **SUMA CAPITAL**.

6. DERECHOS, PRINCIPIOS Y GARANTÍAS

6.1. DERECHOS DEL INFORMANTE

El informante tendrá derecho a:

- Decidir si desea realizar la comunicación de forma anónima o no anónima. En este último caso se garantiza la reserva de la identidad del informante.
- Formular la comunicación verbalmente o por escrito.
- Indicar un lugar donde recibir las comunicaciones: domicilio, correo electrónico, teléfono…
- Renunciar a su derecho a recibir comunicaciones.

Unión Europea	European Anti-Fraud Office (OLAF) https://anti-fraud.ec.europa.eu/index_en
Cataluña	Oficina Antifrau de Catalunya https://www.antifrau.cat/es/investigacion/denuncia.html

- Comparecer ante el Responsable del Sistema interno de información o del Responsable de la Investigación si lo considera oportuno.
- Solicitar que la comparecencia sea realizada por videoconferencia u otros medios telemáticos que garanticen la identidad del informante y la

seguridad y fidelidad de la comunicación.

- Ejercer los derechos que confiere la legislación en materia de protección de datos de carácter personal.
- Comunicar a través del Canal Externo de Información gestionado por parte de la Autoridad Independiente de Protección de Informante cualesquiera acciones u omisiones incluidas en el ámbito de ampliación de este protocolo y de la Ley 2/2023, ya sea directamente o previa comunicación a través del Sistema Interno de Información de la entidad.

6.2. **PRINCIPIOS Y GARANTÍAS**

Todos los miembros de la entidad tienen el derecho y la obligación de informar en el Sistema Interno de Información.

La disponibilidad de acceso al Sistema Interno de Información por parte de los miembros de la entidad como incentivo para el cumplimiento de su deber de comunicación de Infracciones lleva aparejada la necesidad de proteger al informante.

Para ello, en la gestión y tramitación de informaciones, se aplicarán las siguientes garantías:

6.2.1. **Autonomía e Independencia del Responsable del Sistema:** el Responsable del Sistema, así como los demás miembros del Comité de Cumplimiento tienen garantizada su autonomía mediante designación formal, por lo que se comprometen a velar por la confidencialidad y protección del Informante sin admitir presiones ni injerencias de los miembros del Órgano de Administración, ni de cualquier otra área que pudiera resultar implicada por la recepción de una comunicación de infracción.

6.2.2. **Confidencialidad y secretos de las comunicaciones**: Tratamiento confidencial que impida la revelación de datos de carácter personal, así como

cualquier detalle que permitiera la identificación del Informante por parte de las personas o departamentos relacionados con la comunicación, así como por cualquier profesional de la entidad que no sea la Compliance Officer o miembro del Comité de Cumplimiento. La identidad del Informante únicamente podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la Autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.

6.2.3. **Prohibición de Represalias**: La interposición de una comunicación de información realizada con buena fe, con independencia del acierto indagatorio o preventivo de la misma en términos de veracidad, no podrá generar represalia laboral alguna para el Informante. Tampoco podrá generarse presión, en términos de acoso moral o psicológico, con el objetivo de influenciar en el cese de las acusaciones o como venganza por las mismas.

Se trata de un compromiso asumido, mediante la aprobación de este Protocolo, por la Compliance Officer, el Comité de Cumplimiento y el Órgano de Administración. Esta prohibición y la consiguiente protección del Informante por posibles represalias regirá por un periodo de dos años tras la finalización de las diligencias de investigación internas.

6.2.4. **Protección del Informante**: Los miembros del Comité de Cumplimiento y, en especial, el Responsable del Sistema Interno de Información serán los encargados de velar por la protección del Informante, garantizando la no revelación de su identidad y datos personales, así como la ausencia de consecuencias negativas por la interposición de la comunicación de información. En caso de que se requiera al Informante para la aportación de datos o testimonios adicionales de cara a observar la veracidad y gravedad de la comunicación realizada, habrá de hacerse garantizando que tanto en el requerimiento como en la respuesta se mantengan los niveles de protección

antedichos.

6.2.5. **Ausencia de Conflictos de Intereses**: No formará parte de la tramitación e investigación de la comunicación ninguna de las personas relacionadas con la misma.

6.2.6. **Ausencia de Conflictos de intereses en la toma de decisiones del Órgano de Administración:** Se inhibirán de la toma de decisiones para la resolución de la comunicación de información los miembros del Órgano de Administración que pudieran estar afectados por la misma.

6.3. CONFLICTO DE INTERESES

- Las comunicaciones serán recibidas y tramitadas por la Compliance Officer y el Gestor Externo.

- Si las comunicaciones supusieran un conflicto de intereses , que afectase a la Compliance Officer, serán remitidas por el Gestor Externo del Sistema Interno de Información al Comité de Cumplimiento para su tratamiento, quedando apartada del mismo la Compliance Officer.

- De afectar la comunicación de información a algún/os miembro/s del Comité de Cumplimiento, la misma será remitida y tratada con los miembros del Comité no afectados por la misma.

- Si la comunicación de información afecta a todos los miembros del Comité de Cumplimiento, la misma será remitida por el Gestor Externo del Sistema Interno de Información al Consejo de Administración gestionándose con este órgano la investigación y propuesta de actuación.

- Para el caso de que la comunicación de información afecte a todos los miembros del Comité de Cumplimiento, a la Compliance Officer y a algún miembro del Consejo de Administración, será remitida por el Gestor Externo a los miembros del Consejo de Administración no afectados por la comunicación de información y se gestionará con ellos la investigación y la propuesta de actuación.

6.4. **DERECHOS DE LAS PERSONAS INVESTIGADAS**

La Persona investigada tiene derecho a la presunción de inocencia, derecho al honor, al derecho de defensa, de ser informado de las acciones u omisiones que se le atribuyen, debiendo tener acceso al expediente durante la tramitación del mismo y de ser oída en cualquier momento. La comunicación e información referida tendrán lugar en el tiempo y forma que el Responsable de la Investigación considere adecuado para garantizar el buen fin de la investigación.

Asimismo, las Personas investigadas tendrán derecho a la misma protección establecida en este protocolo para los Informantes en relación con la preservación de su identidad y la confidencialidad de los hechos y datos del procedimiento.

El acceso al expediente por parte de la Persona investigada será en relación con los hechos que sean objeto de investigación, sin que sea posible un acceso que permita identificar la identidad del Informante y de los terceros que se mencionen en la información suministrada. De modo que, en cada caso concreto, el Responsable de la Investigación decidirá qué documentos e información es posible compartir con la Persona investigada en caso de que lo solicite.

7. INFORME Y REGISTRO DE LA COMUNICACIÓN DE INFORMACIONES TRAMITADAS

De cada una de las comunicaciones de información se queda un registro en el Sistema Interno de Información numerado en el que se dejará constancia de la recepción de la comunicación, la fecha de interposición, el área de la entidad afectada, la investigación realizada, las acciones llevadas a cabo y las medidas de corrección implementadas. A la información indicada tendrá acceso únicamente la Compliance Officer y el Gestor Externo del Sistema Interno de Información.

La información indicada quedará almacenada de forma indefinida en el sistema con el objetivo de acreditar el funcionamiento del sistema ante una posible investigación judicial como elemento central del Modelo de Prevención de Delitos de la compañía.

8. TRATAMIENTO DE DATOS PERSONALES

El tratamiento de datos personales que deriven de la aplicación de esta política se regirán por lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantías de los derechos digitales, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales y en el TITULO VI de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción por la que se transpone 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.

Los interesados pueden ejercer los derechos recogidos en los art. 11 a 22 del

Reglamento (UE) 2016/679. En concreto, los interesados podrán ejercitar su (i) derecho de acceso, (ii) derecho de rectificación, (iii) derecho de supresión, (iv) derecho de oposición, (v) derecho a la limitación, y, (vi) derecho a la portabilidad de sus datos mediante un escrito identificado con la referencia "Protección de Datos", acompañando su DNI o documento equivalente, por las dos caras, dirigido al Responsable del Tratamiento de los datos de manera presencial o a través del siguiente correo electrónico:dpo@sumacapital.com.

No obstante, en caso de que la persona a la que se refieren los hechos relatados en la comunicación ejerciera el derecho de oposición se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales.

El acceso a los datos contenidos en el Sistema Interno de Información quedará limitado a:

- Gestor externo del Sistema Interno de Información, como encargado del tratamiento de los datos referidos.
- La entidad, como Responsable del Tratamiento de los datos. En este caso, la entidad habilitará el acceso a los datos contenidos en el Sistema Interno de Información al Responsable del Sistema, al Responsable de RRHH cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador o al Responsable de servicios jurídicos de la entidad si procede la adopción de medidas legales en relación con los hechos relatados en la comunicación.
- El Delegado de Protección de Datos, en su caso.

El tratamiento de datos tendrá el siguiente alcance:

- Registro de las comunicaciones recibidas a través de la plataforma online habilitada como Sistema Interno de Información.
- Conservación de los datos recibidos. El plazo de conservación de los datos

será el estrictamente imprescindible para decidir sobre la procedencia de iniciar una investigación, siendo que no podrá exceder de tres meses, ni superar, en ningún caso, los diez años, de conformidad con lo dispuesto en el artículo 26.2 de la Ley 2/2023, de 20 de febrero.

- Supresión de los datos recibidos en los siguientes casos:
    - Transcurridos tres meses desde la recepción de la comunicación sin que se hubiese iniciado actuaciones de investigación, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema.
    - Cuando los datos se refieran a conductas que no consistan ningún tipo de infracción.
    - Cuando la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos.
    - Si se acreditara que la información facilitada o parte de ella no es veraz.

Todos los datos serán tratados con la más estricta confidencialidad, únicamente por el personal autorizado para ello y con la única finalidad de investigar, tramitar y, en su caso, resolver la posible incidencia o irregularidad comunicada.