Stelac

PROCEDIMIENTO DE GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN

[PRC 020]

REGISTRO DOCUMENTAL

RESPONSABLE PROCESO	Responsable del Sistema Interno

FECHA	ESTADO	UNIDAD ORGANIZATIVA
17.01.2024	Elaborado	Cumplimiento Normativo
22.02.2024	Revisado	Responsable del Sistema Interno
27.03.2024	Aprobado	Consejo de Administración

1. CONTROL DE EDICIONES

FECHA	EDICIÓN	CONCEPTO	MODIFICACIÓN REALIZADA
17.01.2024	01	Elaboración de la Política	N/A
27.03.2024	01	Aprobación del Consejo de Administración	N/A

2. NIVEL DE DIFUSIÓN

FECHA	CÓDIGOS DEPARTAMENTOS
27.03.2024	General

ÍNDICE

1. INTRODUCCIÓN

En un compromiso ético y de responsabilidad, Stelac Servicios Financieros, A.V., S.A., en adelante ("la Sociedad") fomenta en su organización una cultura de cumplimiento normativo, ya que las conductas irregulares, perjudican a la organización en particular, y en general al conjunto de la sociedad. Por ello, la Sociedad, buscando prevenir y evitar dichas conductas y proteger a quienes informen sobre ellas de forma eficaz, se ha dotado de un Sistema Interno de Información como instrumento orientado al fortalecimiento de la cultura de la información e integridad y de comunicación de la organización que permita detectar incumplimientos normativos y actos de corrupción conforme a lo dispuesto por 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 (en adelante "Ley 2/2023" o "la Ley") que transpone al ordenamiento jurídico español la Directiva 2019/1937, del Parlamento Europeo y Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (en adelante "la Directiva").

La finalidad de la Ley es la de proteger, frente a posibles represalias, a las personas que, en un contexto laboral o profesional, detecten infracciones u omisiones penales o administrativas graves o muy graves y las comuniquen o informen de las mismas mediante los mecanismos regulados en la misma. Para ello la Ley impone a cualquier entidad obligada por esta ley a disponer de un cauce preferente para informar sobre las acciones e infracciones referidas en la propia ley, denominado en la misma como "Sistema interno de información" (en adelante también "SII"), así como de implantar un del Canal interno de información (en adelante también "CII") y a contar con un procedimiento de gestión de las informaciones recibidas.

Como parte esencial de su Sistema de Información, la Sociedad ha habilitado canales internos de información con la finalidad de posibilitar la comunicación de las infracciones en materia de cumplimiento normativo, fraude y corrupción previstos por la Ley 2/2023 de 20 de febrero por todas las personas establecidas en dicha normativa. En cumplimiento de lo dispuesto por la citada Ley y con la finalidad de asegurar la correcta aplicación y gestión del Sistema y Canal interno de Información el Consejo de Administración de la Sociedad ha aprobado la creación el presente procedimiento de gestión de las informaciones.

2. DEFINICIONES

A los efectos del presente Procedimiento, se entenderá por:

- **Informante:** persona física o jurídica que haya obtenido información sobre acciones u omisiones que puedan constituir infracciones en un contexto laboral o profesional, comprendiendo en todo caso las previstas el punto 4.1., y que las pongan en conocimiento de la Sociedad.
- **Persona afectada o afectado:** persona física a la que se atribuye por el informante la comisión de las infracciones previstas en el punto 4.1. También se considerarán personas afectadas, las que, sin haber sido objeto de información por el informante, a través de los actos de instrucción del procedimiento se haya tenido conocimiento de la presunta comisión por parte de éstas de las infracciones antes referenciadas.
- **Terceros:** personas físicas que pueden tener conocimiento de aspectos relacionados con la infracción informada, ya sea como testigo directo o indirecto y que puede aportar información al procedimiento.
- **Sistema interno de información (SII):** es el cauce de información establecido en la Sociedad para informar sobre las acciones u omisiones constitutivas de infracción previstas en el punto 4.1., con las funciones y contenidos recogidos en punto 6. Incluye el Canal interno de información (punto

6.1) y el Sistema de gestión de la información y Registro de informaciones (procedimiento de gestión en punto 6.4).

- **Canal interno de información (CII):** El canal específicamente habilitado por la Sociedad para recibir la información relacionadas con el objeto de este procedimiento (punto 3.1). Mayor detalle en punto 6.1.
- **Autoridad Independiente de Protección del Informante (AAI):** Constituye el pilar básico del sistema institucional en materia de protección del informante. Autoridad administrativa de ámbito estatal, con personalidad jurídica propia, plena capacidad de actuar de manera pública como privada, que actuará en el desarrollo de su actividad y para el cumplimiento de sus fines con plena autonomía e independencia orgánica y funcional respecto del Gobierno, de las entidades integrantes del sector público y de los poderes públicos en el ejercicio de sus funciones, aunque rinde cuentas de su gestión a congreso y senado. Se relaciona con el Gobierno a través del Ministerio de Justicia, al que está vinculada.

Sus principales funciones, indicadas en la Ley son la gestión del canal externo de información al que puede acudir cualquier informante (punto 6.2), de protección del informante, sancionadoras, consultivas e informativas sobre disposiciones generales en el ámbito de sus competencias y de fomento de la cultura de la información.

3. OBJETIVO

A través de este procedimiento se documentan y establecen las previsiones necesarias para que el Sistema de Información y los canales internos de información a él asociados se adecúen a los requisitos establecidos por la Ley 2/2023 y por la normativa de aplicación en materia de reporte de incumplimientos normativos y corrupción.

El objetivo del Sistema de Información de la Sociedad es el de fortalecer la cultura de información e integridad de la misma, así como el fomento de la cultura de comunicación como mecanismo para prevenir y detectar amenazas al interés público.

El Sistema de información deberá contar con las medidas necesarias para otorgar una protección adecuada frente a represalias a las personas físicas que informen sobre alguna de las infracciones definidas en el apartado 4 y sigan los procedimientos definidos en el presente documento.

4. ÁMBITO DE APLICACIÓN DEL SISTEMA DE INFORMACIÓN

En el presente apartado se establece el alcance del ámbito de protección del Sistema de Información, así como de las medidas de protección establecidos en el mismo.

4.1. ÁMBITO MATERIAL DE APLICACIÓN: Comunicaciones protegidas por el Sistema de Información

El Procedimiento de gestión de informaciones integrado en el Sistema de Informaciones otorgará protección frente a la comunicación de las siguientes infracciones de las que se haya obtenido información en un contexto laboral o profesional:

- Infracciones del Derecho de la Unión Europea conforme a la Directiva UE 1937/2019:
    - Materias de servicios financieros, seguridad en el transporte, protección al medio ambiente o consumidores, salud pública, seguridad alimentaria y bienestar animal, contratación pública y adjudicaciones, enumeradas en el Anexo I;
    - Fraudes que afecten a los intereses financieros de la UE, tal y como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE);
    - Incidan en el mercado interior, como se contempla en el artículo 26.2 del TFUE, incluidas las infracciones de las normas de la U.E. 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.

- Infracciones penales o administrativas graves o muy graves. Se entenderán comprendidas todas las infracciones que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social, así como las relacionadas con acoso definidas en la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva entre mujeres y hombres.

Esta protección no excluirá la aplicación de las normas relativas al proceso penal, incluyendo las diligencias de investigación.

La protección prevista para las personas trabajadoras que informen sobre infracciones del Derecho laboral en materia de seguridad y salud en el trabajo se entiende sin perjuicio de la establecida en su normativa específica.

No dispondrán de las medidas de protección y garantías descritas en este procedimiento:

- Las informaciones que afecten a la información clasificada.
- Las informaciones relativas a infracciones en la tramitación de procedimientos de contratación que contengan información clasificada o que hayan sido declarados secretos o reservados, o aquellos cuya ejecución deba ir acompañada de medidas de seguridad especiales conforme a la legislación vigente, o en los que lo exija la protección de intereses esenciales para la seguridad del Estado.

  En el supuesto de información o revelación pública de alguna de las infracciones a las que se refiere la parte II del anexo de la Directiva, resultará de aplicación la normativa específica sobre comunicación de infracciones en dichas materias.

- Las comunicaciones ya inadmitidas por un canal interno de información de la Sociedad, las que carecieran de toda verosimilizad o que ya estuvieran disponibles para el público o que constituyeran meros rumores.

4.2. ÁMBITO SUBJETIVO DE PROTECCIÓN

El sistema interno de información otorgará protección a las personas físicas que informen sobre infracciones producidas en un contexto laboral y/o profesional:

- Personal vinculado por una relación laboral a la Sociedad.
- Los autónomos que mantengan, o hayan mantenido una actividad profesional con la Sociedad.
- Los accionistas y personas pertenecientes al órgano de administración, dirección o supervisión de la Sociedad, incluidos los miembros no ejecutivos.
- Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores de la Sociedad.
- Informantes que comuniquen información sobre infracciones obtenida en una relación laboral o estatutaria ya finalizada, voluntarios, becarios, trabajadores en periodos de formación perciban o no una remuneración, y aquellos cuya relación laboral todavía no haya comenzado, si la información sobre infracciones ha sido obtenida durante el proceso de selección o de negociación precontractual.

Las medidas de protección del informante previstas en la ley también se aplicarán a:

- Personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso,

- Personas físicas 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. A estos efectos, se entiende que la participación en el capital o en los derechos de voto correspondientes a acciones o participaciones es significativa cuando, por su proporción, permite a la persona que la posea tener capacidad de influencia en la persona jurídica participada.

A nivel general, y salvo las excepciones establecidas en la normativa y en el presente procedimiento, las personas jurídicas no tendrán acceso a las garantías de protección del Sistema de Información.

5. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN.

El Consejo de Administración de la Sociedad ha designado a uno de sus consejeros como Responsable del Sistema Información como figura encargada de asegurar la gestión diligente del sistema. El Responsable del Sistema ejercerá su cargo con independencia del Consejo de Administración habiéndose adoptado las medidas necesarias para asegurar que ejerce sus funciones de forma autónoma e independiente.

El Responsable del Sistema de Información deberá realizar seguimiento de las informaciones comunicadas por el Canal Interno de Información y responderá de la gestión diligente del sistema.

6. IDENTIFICACIÓN DE CANALES

6.1. CANAL INTERNO DE INFORMACIÓN

Con la finalidad de asegurar que el sistema sea gestionado de forma segura, la Sociedad cuenta con los servicios de un aplicativo software informático, para la remisión de comunicaciones. Esta herramienta permite la presentación de informaciones objeto de protección por el presente procedimiento de forma segura, en aplicación tanto de la normativa nacional como la Directiva 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 Responsable del Sistema de Información será la figura encargada de supervisar que las soluciones técnicas utilizadas para el soporte del canal interno de información se adecue a los requisitos mínimos de seguridad y confidencialidad establecidos por la normativa de aplicación y por el presente procedimiento.

El sistema tecnológico adoptado cuenta con medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos de las personas afectadas y cualquier tercero que se mencione en la comunicación. Asimismo, el sistema cuenta con garantías de cumplimiento de protección de la normativa RGPD. Las comunicaciones efectuadas por el canal se encuentran cifradas de extremo a extremo y cuenta con garantías de que no se podrán trazar las direcciones de IP.

El Canal Interno, detallado a continuación, integra los distintos canales internos de información que ya existen dentro de Sociedad, regulados en los procedimientos y políticas internos de la misma, principalmente relativos a la prevención canales de denuncias por conflictos de interés, por operaciones sospechosas por abuso de mercado y uso de información privilegiada y sobre posibles incumplimientos en materia de prevención de blanqueo de capitales y financiación del terrorismo (Manual de prevención del blanqueo de capitales y de la financiación del terrorismo) y posibles infracciones del Reglamento interno de conducta que hace las veces de código ético de la Sociedad.

Para la presentación de informaciones o comunicaciones sobre las irregularidades detectadas indicadas (punto 3.1.) por parte de los informantes (punto 3.2.) se establece el Canal interno de información (CII) que permite la interposición de denuncia de forma telemática y anónima con la inclusión de

documentación, tal como pruebas sobre aquellas conductas que incurren en el incumplimiento de la normativa.

A solicitud del informante, también podrá presentarse mediante una reunión presencial en un plazo máximo de siete días. Esta reunión será documentada. Detalle del funcionamiento del CII y la gestión de la información recibida en punto 7.

Este CII integra los distintos canales internos de información que ya existen dentro de Sociedad, regulados en los procedimientos y políticas internos de la misma, principalmente relativos a la prevención canales de denuncias por conflictos de interés, por operaciones sospechosas por abuso de mercado y uso de información privilegiada y sobre posibles incumplimientos en materia de prevención de blanqueo de capitales y financiación del terrorismo (Manual de prevención del blanqueo de capitales y de la financiación del terrorismo) y posibles infracciones del Reglamento interno de conducta que hace las veces de código ético de la Sociedad.

6.1.1. Procedimiento: Gestión Del Canal Interno De Información

Funcionamiento sobre cómo realizar una comunicación

Para realizar cualquier comunicación se deberá acceder a la dirección web habilitada en la página de inicio de la Sociedad (https://stelac.es/canal-de-denuncias) en una sección separada y presentar la información que se considere necesaria por el informarte para comunicar cualquiera de las infracciones previstas en este procedimiento y la normativa de aplicación.

Se recomienda, en medida de lo posible y a efectos de agilizar los procesos internos de gestión e investigación de comunicaciones, que la información remitida sea lo más descriptiva posible y se aporten aquellos medios de prueba que se consideren convenientes para la investigación y probar los hechos aducidos. Adicionalmente, es recomendable que las comunicaciones estén soportadas por medio de pruebas documentales, siendo también admisibles las pruebas testificales – incluido el testimonio del propio informante- u otros medios de prueba admisibles en derecho, si bien su no aportación no supondrá por defecto su inadmisión.

También podrá presentarse, a solicitud del informante, mediante una reunión presencial dentro del plazo máximo de siete días, solicitándolo en la comunicación inicial. Estas reuniones, previo consentimiento del informante, serán documentadas a través de una transcripción completa y exacta de la conversación realizada. Se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma dicha transcripción.

Una vez realizada la comunicación, el sistema facilitará al informante un Código de Identificación al objeto de procurar el contacto entre la Sociedad y el informante aun cuando se hubiera optado por el anonimato en la comunicación.

Cuando la información no se remita a través del Canal Interno y llegue a miembros de la Sociedad distintos del Responsable del Sistema, éstos tienen la obligación de remitírsela con carácter inmediato al mismo, así como el deber de preservar la confidencialidad y abstenerse de realizar cualquier actuación que pueda revelar directa o indirectamente la identidad del informante y de la persona afectada. La divulgación por parte del tercero receptor de la mera existencia y, en su caso, del contenido de la información, puede suponer la vulneración de las garantías de confidencialidad y anonimato, conducta tipificada como infracción muy grave en el artículo 63.1.c) de la Ley 2/2023 de 20 de febrero.

Destinatarios del canal

La Sociedad cuenta con los servicios de gestión del Sistema Interno de información por tercero externo, el cual será el responsable de la recepción inicial, clasificación y revisión de admisión a trámite de las

comunicaciones recibidas. Asimismo, el Responsable del Sistema de Información también tendrá acceso al canal interno de información.

En el caso de que la información se refiera a cualquiera de los destinatarios del canal interno de información se deberán establecer sistemas orientados a evitar que las personas afectadas accedan a la información.

Requisitos formales de la comunicación

La comunicación deberá contener al menos los siguientes requisitos:

- Identificación del informante (salvo que se presente la información anónimamente).
- Descripción de los hechos
- Identificación de la persona o personas afectadas
- Identificación, en su caso, de terceros que puedan aportar información relevante.
- Si se ejerce el derecho a renunciar a comunicarse con el RSII.

Al presentar la información, si no ejerce dicha renuncia, el informante podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las comunicaciones como el acuse de recibo etc. El mail en ningún caso se utilizará para solicitar información confidencial.

En caso de apreciarse por el RSII la falta de alguno de los requisitos que se acaban de indicar, se procederá en la medida de lo posible, a solicitar la subsanación.

Acuse de recibo

Tras la recepción de la comunicación, el Responsable del Sistema de información deberá remitir acuse de recibo al informante en un plazo no superior a 7 días naturales, contados a partir de la fecha de la comunicación. No se acusará recibo de la comunicación para aquellos casos que, de forma motivada se considere que dicho acuse de recibo puede poner en peligro la confidencialidad de la comunicación.

Con el acuse de recibo, se remitirá al informante la siguiente información al informante:

- Información clara y accesible sobre sobre los canales externos de información ante las autoridades competentes, así como antes las instituciones, órganos u organismos de la Unión Europea a lo dispuesto por el Anexo II.
- Política de Privacidad en materia de Protección de datos de la Sociedad
- Información sobre que su identidad será en todo caso reservada y no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.
- Información relativa al tratamiento de datos de carácter personal de conformidad con lo dispuesto en el RGPD.
  Respecto de los terceros que comparezcan presencialmente, se les proporcionará, en el momento de dicha comparecencia, la información relativa al tratamiento de sus datos de carácter personal de conformidad con lo dispuesto en el RGPD.
- Información sobre la posibilidad de presentar la información ante la AAI.

Se informará de forma expresa al informante que su identidad será en todo caso reservada y que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.

Admisión a trámite

Recibida la comunicación, el Responsable del Sistema procederá a la valoración de la admisibilidad de la comunicación, para evaluar si la información se ajusta al ámbito de aplicación material indicado en el apartado 4.1. del presente documento y es presentada por persona con acceso de acuerdo con lo

establecido en el apartado 4.2. Como resultado de este análisis inicial resolverá inadmitir la comunicación, si no se ajusta al ámbito previsto antes mencionando, o admitirla a trámite.

El Responsable del Sistema de Información deberá comunicar al informante la admisión a trámite del procedimiento de investigación, o en su caso su inadmisión.

En el caso de que por falta de elementos de prueba no se pueda continuar con el proceso de investigación, se deberá comunicar dicha circunstancia al informante al objeto de requerirle la remisión de información adicional. En caso de que esta no sea facilitada en un plazo de 10 días, se comunicará al informante la imposibilidad de continuar con la investigación procediendo a la finalización y archivo de la comunicación.

Aún en el caso de que se decida no admitir a trámite la investigación, se deberá guardar registro de la comunicación.

En caso de admisión, se iniciarán las diligencias de análisis a practicar o instrucción, entre las que se encuentran la interacción con las partes interesadas y las comunicaciones y cumplimiento de los requisitos en materia de protección de datos personales. En caso de inadmisión, se finalizará la gestión del expediente y así se comunicará al informante.

Se remitirá con carácter inmediato la información al Ministerio Fiscal cuando los hechos pudieran ser indiciariamente constitutivos de delito, o a la Fiscalía Europea en el caso de que los hechos afectan a los intereses financieros de la Unión Europea. En este caso, se producirá la finalización del procedimiento haciendo constar en el registro del mismo esta circunstancia.

6.2. FASE DE INSTRUCCIÓN Y ESTUDIO

Desde la recepción de la comunicación, y en caso de admisión a trámite, se iniciará el proceso de investigación, debiendo seguirse lo establecido en el procedimiento interno de investigación establecido por la Sociedad.

Conforme a lo dispuesto por la normativa de aplicación el plazo máximo para la resolución y respuesta a las actuaciones de investigación será de 3 meses desde la remisión del acuso de recibo. Dicho plazo podrá ser ampliado por otros 3 meses adicionales para aquellos casos que sean considerados de especial complejidad.

La instrucción, llevada a cabo por el Responsable del Sistema, comprenderá todas aquellas actuaciones encaminadas a comprobar la verosimilitud de los hechos relatados. Los actos de instrucción se realizarán de modo que se garanticen los derechos fundamentales del informante y del afectado.

Las comunicaciones que se realizan con la persona afectada, así como todos los actos en esta fase de instrucción, se documentan en el sistema de gestión de la información y se deja constancia de su resultado, tanto si han sido recogidas expidiéndose el correspondiente acuse de recibo, como si han sido rehusadas en el Registro de informaciones. El afectado no tiene obligación de declarar ni de cumplir los requerimientos que el RSII, sin perjuicio de la constancia de esta circunstancia en el expediente.

6.2.1. Información al Afectado

En el plazo máximo de 15 días laborables desde la resolución de admisión, se dará conocimiento al afectado de la existencia de las actuaciones, de los hechos relatados de manera sucinta, salvo que dicha comunicación pueda facilitar la ocultación, destrucción y alteración de pruebas, en cuyo caso, el responsable del Sistema, podrá modificar dicho plazo hasta que desaparezcan dichas circunstancias.

Además, se le informará del derecho que tiene a presentar alegaciones por escrito y aportar las pruebas que considere, a solicitar una entrevista con el Responsable del Sistema y del tratamiento de sus datos personales.

En ningún caso se comunicará al sujeto afectado la identidad del informante ni se le dará acceso a la comunicación. Se advertirá al afectado de las consecuencias de revelar información a terceros en los términos previstos en la Ley 2/2023.

6.2.2. Trámite de Audiencia

Recibida la comunicación indicada en el punto anterior, el afectado podrá presentar alegaciones y la documentación que estime conveniente en el plazo de 15 días laborables.

Si el Responsable del Sistema considera conveniente realizar una entrevista, o la solicita el afectado, el Responsable del Sistema fija la misma con indicación de lugar, fecha y hora y se lo comunicará al afectado. Sin perjuicio de lo indicado anteriormente, el afectado tiene derecho a ser oído en cualquier momento.

Las comunicaciones y entrevistas se realizarán con la máxima discreción posible, con la finalidad de preservar el secreto de las actuaciones, preservando la identidad del informante, terceros y afectados, y, en todo caso, garantizando la confidencialidad de las informaciones.

Si durante la instrucción del procedimiento se apreciase que los hechos pudieran revestir el carácter de delito, el Responsable del Sistema remitirá las actuaciones al Ministerio Fiscal y emitirá un informe en el que se recoja expresamente esta circunstancia y la finalización del procedimiento.

6.2.3. Acceso al Expediente

En cualquier momento durante la tramitación del procedimiento, el informante y el afectado tendrá derecho a acceder al contenido del expediente, siempre que dicho acceso no facilite la ocultación, destrucción y alteración de pruebas, en cuyo caso el Responsable del Sistema podrá diferir el acceso de forma motivada, hasta que desaparezcan dichas circunstancias. El Responsable del Sistema adoptará las medidas necesarias para que el acceso se produzca preservando la identidad del informante.

En el caso de que se proceda al acceso al expediente quedará constancia de ello en el sistema de gestión de la información, con indicación del contenido, fecha y hora en el Registro.

El afectado tiene el deber de mantener la confidencialidad de la información a la que tenga conocimiento como consecuencia del acceso al expediente. Queda prohibida cualquier actuación tendente a identificar al informante o terceros.

6.3. FINALIZACIÓN DEL PROCESO INTERNO

Admitida a trámite la comunicación y tras su estudio, el Responsable del Sistema emitirá un informe, y se notificará al informante, en la medida en que este identificado y no haya hecho uso del derecho a renunciar a comunicarse con el Responsable del Sistema, y a la persona afectada.

Emitido el informe, el Responsable del Sistema adoptará alguna de las siguientes decisiones con el expediente:

- El archivo del mismo
- Su remisión al Ministerio Fiscal o Fiscalía Europea si hubiera indicios de delito.
- La comunicación de la información a la autoridad competente o a la AAI si estimara que los hechos comunicados podrían ser constitutivos de falta grave o muy grave.

  En este último caso, el Responsable del Sistema traslada la información obtenida y el resultado de su análisis a la autoridad competente mediante un procedimiento que garantice la confidencialidad de la identidad del informante y de información trasladada.

En cualquier caso, el Responsable del Sistema deberá dar respuesta a las actuaciones de investigación en un plazo que no podrá ser superior a tres meses desde la recepción de la comunicación o, si no se remitió 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 tres meses adicionales.

6.4. REGISTRO DE LA INFORMACIÓN

El sistema de gestión de información estará contenido en un Registro de informaciones que es una base de datos segura y de acceso restringido al Responsable del Sistema, en la que se registrarán todas las comunicaciones recibidas con al menos los siguientes datos:

a) Fecha de recepción
b) Código de Identificación
c) Actuaciones desarrolladas
d) Medidas adoptadas
e) Fecha de cierre

Sin perjuicio del Registro de informaciones mencionado anteriormente, la presentación de información se documentará, en su caso:

1. Mediante la copia del escrito de presentación de la información
2. A través de la transcripción completa y exacta de la conversación mantenida en la reunión presencial, si esta se ha dado.

El Responsable del Sistema garantiza desde el principio del proceso la confidencialidad del interlocutor y la protección de sus datos de carácter personal. El sistema no almacenará datos personales que no sean imprescindibles para el conocimiento y tratamiento de la información recibida. El RSII suprimirá los datos personales no necesarios.

Este registro no será público y solo se podrá acceder a él mediante petición razonada de la Autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquella.

Los datos personales relativos a las informaciones recibidas y a las gestiones del Responsable del Sistema solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con la Ley 2/2023.

El Responsable del Sistema eliminará estos datos personales tras un plazo establecido (en todo caso inferior a un año) tras lo cual sólo quedará la información de carácter no personal en el Libro del Registro de informaciones a efectos de control de actuaciones y estadísticos.

7. DERECHOS DEL INFORMANTE

Los principales derechos del informante, al margen de lo indicado en la Ley 2/2023 son:

1. Puede elegir libremente el canal, interno o externo, al que dirigir su comunicación.
2. En el caso del CII de la Sociedad, podrá presentar la información mediante por vía postal o, si así lo solicitara, presencialmente.
3. A comparecer ante el RSII por iniciativa propia.
4. Podrá presentar la comunicación de forma anónima, por tanto, derecho a preservar su identidad.
5. A la protección de sus datos personales.
6. A indicar un domicilio, mail o lugar seguro donde recibir las comunicaciones del RSII.
7. La confidencialidad de sus datos y comunicaciones está garantizada durante todo el proceso de gestión de la información presentada.

8. También tiene derecho a renunciar a que se le envíen comunicaciones posteriores a la presentación de la información.
9. Salvo que renuncie de forma expresa a recibir comunicaciones o que presente su comunicación anónimamente, tiene derecho a conocer el estado de la tramitación de su comunicación y el resultado final de la actuación del RSII en los plazos fijados.
10. Las personas que comuniquen o revelen infracciones previstas en ámbito de aplicación de la Ley 2/2023 tendrán derecho a protección siempre que:
    a. tengan motivos razonables para pensar que la información es veraz en el momento de la comunicación, aun cuando no aporten pruebas concluyentes, y que esta información entra dentro del ámbito de aplicación de esta ley.
    b. la comunicación se haya realizado conforme a los requerimientos previstos en la ley.

La Ley prohíbe expresamente los actos constitutivos de represalia contra el informante, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación conforme a lo previsto en ella, siendo estos catalogados como infracción muy grave en el artículo 63 de la Ley. Se consideran represalias, entre otros, la suspensión del contrato de trabajo, despido o extinción de la relación laboral, degradación o denegación de ascenso, intimidación, acoso, discriminación, o trato desfavorable o injusto. Mayor detalle de las represalias prohibidas y medidas de protección al informante en Título VII de la Ley.

A los terceros en el procedimiento se les reconocen los derechos previstos en los puntos 2,4,5,6 y 7 anteriores. Sin perjuicio de la posibilidad de extender a éstos, y en la medida de lo posible, las medidas de apoyo y protección del informante previstas en la Ley 2/2023.

8. DERECHOS DE LAS PERSONAS AFECTADAS

Las personas afectadas tienen los derechos que les reconozcan la Constitución y las leyes, debiendo estar garantizados por el Responsable del Sistema, y en especial los siguientes:

1. A ser informadas a la mayor brevedad posible de la información que les afecta, y a ser oídas en cualquier momento.
2. A la presunción de inocencia
3. Al honor y a la intimidad
4. Derecho de defensa, usando los medios válidos en derecho para la misma y a ser asistidas por abogado.
5. Derecho de acceso al expediente en los términos regulados en la ley, con acceso a las actuaciones que se siguen contra ellas, sin perjuicio de las limitaciones temporales que se pueden adoptar para garantizar el resultado de las actuaciones.
6. A la preservación de su identidad, frente a cualquier persona ajena al Responsable del Sistema
7. A la protección de sus datos personales
8. A la confidencialidad de las comunicaciones, hechos y datos del procedimiento

Se informará a las personas afectadas por las comunicaciones realizadas en los canales internos de información, sobre las acciones u omisiones que se le atribuyen, de su derecho a ser oídas, así como de los derechos que le asisten, en un plazo y forma que se considere más adecuada para garantizar el buen fin de la investigación.

La persona afectada por la información tendrá derecho de acceso al expediente. En caso de solicitarlo, toda información personal o datos de terceros, como el informante, testigos u otras personas mencionadas, deberá eliminarse de los documentos. En los supuestos en que, por la naturaleza de la información o los hechos descritos en ella, la identidad del informante o de terceros fuese obvia o fácilmente identificable, se podrá aplazar el derecho de acceso al expediente del informante, hasta que se

tomen las garantías necesarias para asegurar la confidencialidad de la identidad del informante o los terceros.

9. GARANTÍA DE CONFIDENCIALIDAD EN EL CASO DE COMUNICACIONES POR MEDIOS AJENOS AL CANAL INTERNO

En el caso de que se remitan fuera de los canales internos de información comunicaciones dentro del alcance establecido por el presente procedimiento, las personas receptoras de la comunicación deberán guardar confidencialidad sobre la información recibida y comunicarla de forma inmediata al Responsable Interno de la Información.

El incumplimiento de esta obligación supondrá una infracción muy grave conforme a lo establecido por la Ley 2/2023 de 20 de febrero.

La Sociedad cuenta con medidas organizativas internas orientadas a asegurar que todo su personal ha sido formado sobre la obligación establecida en el presente artículo.

10. INFRACCIONES-RÉGIMEN SANCIONADOR

La AAI es el órgano competente para el conocimiento de las infracciones contempladas en el título IX de la Ley 2/2023.

Entre dichas infracciones se tipifican, entre otras, la adopción de cualquier represalia derivada de la comunicación frente a los informantes, la vulneración de las garantías de confidencialidad y anonimato previstas en la Ley, del deber de mantener secreto sobre cualquier aspecto relacionado con la información, y comunicar o revelar públicamente información a sabiendas de su falsedad.

11. GARANTÍAS DEL SISTEMA DE INFORMACIÓN

El Sistema de Información ha sido configurado para la garantizar la confidencialidad de la identidad de la persona informante, así como de cualquier otra persona mencionada en la comunicación. El sistema de información está configurado para no obtener datos de las personas que realicen comunicaciones.

Asimismo, se han establecido medidas para garantizar la seguridad y confidencialidad en la gestión de comunicaciones y procedimientos internos de investigación. La información de la comunicación sólo se revelará a quienes sea estrictamente necesario para la gestión de la investigación de acuerdo con la normativa de aplicación.

Únicamente se podrá revelar la identidad de la persona informante fuera del procedimiento interno de investigación en caso de comunicación a la Autoridad Judicial, Ministerio Fiscal o autoridad administrativa competente en el marco de una investigación penal o sancionadora. En estos supuestos, se indicará dicha cesión al informante antes de revelar su identidad, salvo que pudiera comprometer la investigación o procedimiento judicial.

El libro registro de las informaciones recibidas e investigaciones 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

11.1. GARANTÍA DE NO REPRESALIAS Y PROTECCIÓN AL INFORMANTE

El Consejo de Administración de la Sociedad prohíbe expresamente los actos constitutivos de represalia, incluidas las amenazas y tentativas de represalia, contra las personas que presenten una comunicación o que comuniquen o revelen públicamente informaciones conforme a los requisitos de protección previstos en la Ley 2/2023 de 20 de febrero.

Se entiende por represalia cualesquiera actos u omisiones prohibidos por la Ley 2/2023, 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.

A título enunciativo se consideran represalias las siguientes:

- 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.
- Daños, incluidos de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo
- Evaluación o referencias negativas respecto al desempeño laboral o profesional
- Inclusión de listas negras o difusión de información que dificulte o impidan el acceso al empleo o la contratación de obras o servicios.
- Denegación de formación
- Discriminación, o trato desfavorable o injusto

Conforme a lo establecido por la normativa de aplicación, no se considerará que las personas físicas que comuniquen información sobre acciones u omisiones recogidas por la Ley 2/2023 hayan infringido ninguna restricción de revelación de información, y no incurrirán en responsabilidad de ningún tipo en relación a dicha comunicación, siempre que tuvieran motivos razonables para para pensar que la información comunicada es veraz en el momento de la comunicación y que la citada información entré dentro del ámbito de aplicación de la Ley. Esta medida no afectará a las responsabilidades de carácter penal.

El Responsable del Sistema Interno de Información del Club deberá asegurar que ninguna de las personas que comuniquen a través del sistema interno de información, canales externos de información o incluso a través de revelación pública en cumplimiento de los requisitos de la normativa sean objeto de cualquier tipo de represalia.

11.2. PRESUNCIÓN DE INOCENCIA

Durante la tramitación de la investigación las personas afectadas por la comunicación tendrán derecho a la presunción de inocencia, al derecho de defensa y al acceso al expediente en los términos regulados en este procedimiento y la Ley 2/2023 de 20 de febrero.

Asimismo, las personas afectadas por comunicaciones tendrán la misma protección que la prevista para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

12. PROTECCIÓN DE DATOS PERSONALES

El tratamiento de datos personales obtenidos a través del SII se regirá por 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 (también “Reglamento general de protección de datos” o “RGPD”); en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; y en el título VI de la propia Ley 2/2023. Mayor detalle de protección de datos personales en poder de la Sociedad su procedimiento “PRC 009 Protección de Datos de carácter personal”.

El RSII es el encargado del tratamiento de los datos recibidos a través del CII y el órgano de administración el responsable del tratamiento de los datos personales recibidos.

El SII impide el acceso no autorizado y preserva la identidad y garantiza la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado.

La identidad del informante solo 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, y estos casos estarán sujetos a las salvaguardas establecidas en la normativa aplicable.

Si la información recibida contuviera categorías especiales de datos, se procederá a su inmediata supresión, salvo que el tratamiento sea necesario por razones de un interés público esencial según lo previsto en el RGPD, según dispone el artículo 30.5 de la Ley.

No se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una información específica o, si se recopilan por accidente, se eliminarán sin dilación indebida.

En todo caso, transcurridos 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.

13. PUBLICIDAD

La Sociedad facilitará a todas las personas interesadas la información adecuada y de d forma fácilmente accesible sobre el uso del Sistema interno de información implantado en su organización, y los principios esenciales del procedimiento de gestión de las comunicaciones realizadas.

La persona responsable del sistema deberá dar cumplimiento a las obligaciones de publicación.

Dicha información queda accesible a través del presente documento, y disponible para su consulta en la página web de la Sociedad en la siguiente dirección:

https://stelac.es/m-i-f-i-d-ii

14. NORMATIVA DE APLICACIÓN

Las principales normas que se aplican en este procedimiento son:

- 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.
- 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.
- Ley 35/2003, de 4 de noviembre, de Instituciones de Inversión Colectiva.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva entre mujeres y hombres.
- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 6/2023, de 17 de marzo, de los Mercados de Valores y de los Servicios de Inversión.

ANEXO I – HECHOS COMUNICABLES A TRAVÉS DEL CANAL INTERNO DE INFORMACIÓN

ORDENAMIENTO JURÍDICO	SECTOR	ÁMBITO DE LAS INFRACCIONES
Ordenamiento jurídico español	Penal	Infracciones graves o muy graves
	Administrativo	Infracciones graves o muy graves
Derecho de la UE	Intereses financieros de la UE (art. 325 TFUE)	Fraude y actividades ilegales
	Mercado interior (art. 26.2. TFUE)	Infracciones del mercado interior relativas a la libre circulación de mercancías, personas, servicios y capitales
		Infracciones de las normas de la UE en materia de competencia y ayudas otorgadas por los Estados
		Infracciones de las normas del impuesto sobre sociedades. Prácticas encaminadas a obtener ventajas fiscales que desvirtúen la finalidad del impuesto de sociedades
Derecho de la Unión Europea. Ámbitos específicos del Anexo de la Directiva 2019/1937	Contratación pública	Contratación pública
	Adjudicaciones	Adjudicaciones de concesiones
		Adjudicaciones de contratos en los ámbitos de seguridad
		Adjudicación de contratos por entidades de los sectores de: agua, energía, transportes, servicios postales
	Servicios, productos y mercados financieros, y prevención del blanqueo de capitales y financiación del terrorismo.	Normas que establecen un marco regulador y de supervisión y protección para los inversores y consumidores en los servicios financieros y mercados de capitales de la Unión, los productos bancarios, de crédito, de inversión, de seguro y reaseguro, de pensiones personales y de jubilación, servicios de valores, de fondos de inversión y de pago
	Seguridad de los productos y conformidad	En empresas de fabricación y distribución posibles prácticas abusivas e ilícitas de fabricación, importación o distribución relativas a productos inseguros
	Seguridad del transporte	Requisitos de seguridad en el transporte ferroviario, sector de la aviación civil, transporte por carretera, sector marítimo, transporte terrestre de mercancías peligrosas
	Protección del medio ambiente	Infracciones cometidas contra la protección del medio ambiente, ya que provocar perjuicios para el interés público y posibles efectos colaterales más allá de las fronteras nacionales. Las normas establecidas para la protección del medio ambiente engloban los siguientes ámbitos: medio ambiente y clima,

		desarrollo sostenible y gestión de residuos, contaminación marina, atmosférica y sonora, gestión de aguas y suelos, naturaleza y biodiversidad, sustancias y mezclas químicas, y los productos ecológicos
	Protección frente a las radiaciones y seguridad nuclear.	Seguridad nuclear, la protección frente a las radiaciones y la gestión responsable y segura del combustible que se consume, además de los residuos radiactivos
	Seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales	Se pretende la denuncia de infracciones en estos ámbitos para asegurar la protección de la salud humana, los intereses del consumidor en relación a estos alimentos que consume y el funcionamiento eficaz del mercado interior.
	Salud pública	Para preservar la calidad y seguridad de los órganos y las sustancias de origen humano, medicamentos y productos de uso médico y derechos de los pacientes
	Protección de los consumidores	Vinculada a casos en los que los productos no seguros pueden causar importantes perjuicios a los consumidores
	Protección de la privacidad y de os datos personales, y seguridad de las redes y los sistemas de información	Infracciones contra la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información, que puedan ocasionar daños de interés público

ANEXO II - CANALES EXTERNOS DE INFORMACIÓN

Toda persona física que forme parte de algunos de los colectivos con acceso al Sistema Interno puede dirigirse al canal externo gestionado por la AAI (regulado en la Ley 2/2023 en su título III) o ante los canales análogos de las autoridades u órganos autonómicos correspondientes, ya sea directamente, ya con posterioridad a la previa comunicación de información ante el Canal Interno, para informar de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación material de la Ley 2/2023. Este canal externo es:

- Canal establecido por la AAI (órgano estatal vinculado al Ministerio de Justicia)

  A especificar una vez la Autoridad Independiente de Protección al Informante se encuentre operativa.

- Canal establecido por la Comunidad de Madrid (órgano autonómico).

  https://www.comunidad.madrid/transparencia/canal-del-informante

Existen otros canales externos de organismos para comunicar información sobre las infracciones recogidas en el ámbito material de aplicación de la Ley 2/2023. Los principales son:

- Banco de España:

  https://www.bde.es/bde/es/secciones/sobreelbanco/Transparencia/Informacion_inst/registro-de-acti/Canal_de_denuncias.html

- Comisión Nacional de los Mercados de Valores (CNMV):

  https://www.cnmv.es/portal/whistleblowing/presentacion.aspx

- SEPBLAC:

  https://www.sepblac.es/es/sujetos-obligados/tramites/comunicacion-por-indicio/

- Agencia Española de Protección de Datos

  https://whistleblowersoftware.com/secure/aepd-canal-proteccion-informante/9950b8af-daf7-493b-92ae-6eb1c7962d99

- Agencia Tributaria

  https://sede.agenciatributaria.gob.es/Sede/colaborar-agencia-tributaria/denuncias.html

- Comisión Nacional de los Mercados y la Competencia (CNMC):

  https://sede.cnmc.gob.es/tramites/competencia/denuncia-de-conducta-prohibida

- Autoridad Independiente de Responsabilidad Fiscal

  https://www.airef.es/es/canal-de-denuncias/

- Oficina Europea Antifraude:

  https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_es

  https://fns.olaf.europa.eu/main_es.htm

- Canal Externo de la Unión Europea:

https://european-union.europa.eu/contact-eu/make-complaint_es

- Infofraude (Hacienda-Gobierno de España):

  https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/paginas/denan.aspx

A través de nuestra página web, le informaremos de las actualizaciones que puedan producirse en lo referente a canales externos de información y la creación de canales externos de comunicación de la Autoridad Independiente de Protección al Informante A.A.I.