

Política del Sistema Interno de Información

LIFT INVESTMENT ADVISORS EAF

Índice

0.	Introducción y objeto de la política.....	3
1.	Normativa de referencia	3
2.	Ámbito de aplicación.....	3
2.1.	Ámbito subjetivo de aplicación	3
2.2.	Ámbito objetivo de aplicación.	4
3.	Responsable del sistema interno de información	4
4.	Principios generales de actuación y garantías del sistema	5
5.	Canal de Denuncias interno.....	7
6.	Canales de Denuncias externos	7
7.	Tratamiento de datos de carácter personal	7
8.	Aprobación, revisión y publicidad de la política	8

0. Introducción y objeto de la política

De conformidad con lo dispuesto en 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 y su transposición al ordenamiento español, mediante la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, las entidades del sector privado sujetas al ámbito de aplicación de la normativa de prevención del blanqueo de capitales o de la financiación del terrorismo, deben contar con un canal interno de información.

En cumplimiento de dicha obligación, LIFT INVESTMENT ADVISORS EAF (en adelante, "LIFT", o la "Entidad", o la "Sociedad") ha elaborado la presente Política del Sistema Interno de Información (la "Política") que desarrolla los principios básicos del sistema interno de información o Canal de Denuncias de la Entidad.

La finalidad de este sistema es 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 LIFT.

1. Normativa de referencia

- Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.
- Ley 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").
- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo ("Ley 10/2010").
- Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros ("MiFID II").
- 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").
- Reglamento 596/2014 del parlamento europeo y del consejo de 16 de abril de 2014 sobre el abuso de mercado ("Reglamento de Abuso de Mercado").

2. Ámbito de aplicación

2.1. Ámbito subjetivo de aplicación

El ámbito subjetivo de aplicación de la Política es todos los empleados, altos directivos, miembros del consejo de administración de LIFT (en adelante, "**Personas Sujetas**").

Asimismo, también podrán utilizar este sistema cualquier persona que trabaje para o bajo la supervisión de los proveedores de la Sociedad.

Igualmente lo podrán utilizar todas aquellas personas que mantuvieron con LIFT 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 aquellas 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.

2.2. Ámbito objetivo de aplicación.

A través de los hechos comunicados en el Canal de Denuncias se puede dar a conocer, cualquier posible irregularidad o acto que se sospeche o conozca que son indebidos o contrarios a la legislación vigente o a la normativa interna de LIFT, cometidos en el seno de la Entidad o de su actividad.

En concreto, podrán informar sobre las infracciones contenidas en el artículo 2 de la Ley 2/2023, esto es, aquellas que:

- puedan constituir infracciones del Derecho de la UE siempre que entren dentro del ámbito de aplicación enumerado en el anexo de la Directiva 2019/1937 y que afecten a los intereses financieros de la UE o incidan en el mercado interior. Entre las cuestiones que se encuentran detalladas en el anexo de la citada Directiva se encuentran:
 - servicios, productos y mercados financieros,
 - prevención del blanqueo de capitales y de la financiación del terrorismo,
 - protección de los inversores y consumidores,
 - protección de la privacidad y de los datos personales, y seguridad de las redes y de los sistemas de información,
- puedan ser constitutivas de infracción penal o administrativa grave o muy grave. En todo caso, se entenderán comprendidas todas aquellas infracciones penales o administrativas graves o muy graves que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.
- puedan ser constitutivas de infracciones de las políticas y procedimientos internos de la Entidad.

3. Responsable del sistema interno de información

El Consejo de Administración de la Entidad nombrará a un Responsable del Sistema Interno de Información que, en todo caso, tendrá un cargo directivo.

Este responsable actuará con autonomía e independencia del resto de órganos de la Entidad.

Además de este responsable, únicamente accederán a las denuncias aquellas personas que, por el desarrollo de sus funciones en la Entidad, debieran tener acceso a ellas, como son aquellas personas de las funciones de control necesarias para su efectiva tramitación.

Asimismo, excepcionalmente, podrán acceder a las denuncias las personas con funciones de gestión y control de recursos humanos en la Entidad, en el caso concreto de que fuera necesario proceder la adopción de medidas disciplinarias contra una Persona Sujeta.

Por otro lado, la Entidad cuenta con un Delegado de Protección de Datos que revisará los tratamientos llevados a cabo.

4. Principios generales de actuación y garantías del sistema

Los principios generales de actuación del Sistema Interno de Información son los siguientes:

- **Confidencialidad:** El sistema interno de información garantizará la confidencialidad en relación con la identidad del informante, las personas mencionadas en la comunicación, la información comunicada y las actuaciones que se desarrollen a consecuencia de la tramitación de la comunicación.

En todo caso, en el proceso de investigación se seguirán las previsiones de la normativa en materia de protección de datos, especialmente en lo referente a la identidad del informante o cualquier otra información relacionada con datos personales. Asimismo, cualquier dato de carácter personal que no fuera necesario para la efectiva investigación y tramitación de las denuncias no será recopilada y, en su caso, se eliminará sin dilación indebida en caso de que fueran recopilados por accidente.

- **Anonimato:** Se facilitará a los informantes un canal que les permita la presentación de denuncias de manera anónima en caso de que el denunciante así lo eligiera.
- **Independencia y autonomía:** En la tramitación del procedimiento se evitará en todo momento cualquier situación que pueda suponer un potencial conflicto de interés, garantizando así la independencia e imparcialidad del Responsable del Sistema Interno de Información así como de cualquier persona dentro del personal que pudiera intervenir en él.

Además, en el sistema interno de información se garantizarán los siguientes derechos:

- **Protección a los informantes:** Se garantizará un sistema de protección a los informantes frente a posibles represalias. Por ello, se prohíben expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación conforme a lo previsto en el Procedimiento del Sistema Interno de Información.

Es decir, las personas que denuncien posibles infracciones tendrán derecho a protección siempre que tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación o revelación, aun cuando no aporten pruebas concluyentes.

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, sólo por su condición de informantes, o por haber realizado una revelación pública. Se exceptúa el supuesto en que dicha acción u omisión pueda justificarse objetivamente en atención a una finalidad legítima y que los medios para alcanzar dicha finalidad sean necesarios y adecuados.

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

- 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.

- o Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.
- o Evaluación o referencias negativas respecto al desempeño laboral o profesional.
- o 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.
- o Denegación o anulación de una licencia o permiso.
- o Denegación de formación.
- o Discriminación, o trato desfavorable o injusto.

El denunciante 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.

- **Derechos a la presunción de inocencia y al honor:** Se garantiza la presunción de inocencia y al honor de las personas afectadas, así como el derecho a ser escuchadas.
- **Derecho de información:** Las personas que puedan verse afectadas por una investigación interna tienen el derecho a tener conocimiento de la comunicación formulada en su contra tan pronto como se hayan realizado las comprobaciones oportunas, se haya admitido a trámite el expediente y se considere adecuado para garantizar el buen fin de la investigación.

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 Canal de Denuncias 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 denunciante 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 Canal de Denuncias, podrán evitar comunicar dicha información al denunciante hasta el momento del trámite de audiencia.

Asimismo, de acuerdo con lo exigido por el RGPD, el denunciante podrá ejercer sus derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento y portabilidad obtenidos a través de este Canal poniéndose en contacto con el responsable de seguridad, a través del correo electrónico del delegado de protección de datos: rgpd@auratechlegal.es

- **Conservación de los registros:** Todas las denuncias y consultas que se reciban por el Canal de Denuncias, 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 la Entidad de acuerdo con lo dispuesto en la normativa aplicable en materia de protección de datos personales y durante el tiempo estrictamente necesario a los efectos de desarrollar la investigación o para aplicar las medidas oportunas a los efectos de defender los intereses de la Entidad. En ningún caso podrán conservarse los datos por un período superior a diez(10) años.

Los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el Canal de Denuncias 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 introducción de los datos, deberá procederse a su supresión. 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.

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 Canal de Denuncias.

5. Canal de Denuncias interno

La Entidad dispone de los siguientes medios a través de los cuales podrán comunicarse los hechos y conductas denunciables descritas en el apartado 4:

- A través de la página web en el apartado establecido para ello

A petición del informante, la comunicación de los hechos denunciables también se puede hacer mediante reunión presencial, tras la solicitud formal por escrito. Las comunicaciones verbales realizadas a través de reunión presencial deberán documentarse de alguna de las maneras siguientes, previo consentimiento del informante:

- mediante una grabación de la conversación en un formato seguro, duradero y accesible, o
- a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.

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

6. Canales de Denuncias externos

Los supervisores según el ámbito normativo cuentan con canales específicos donde podrán presentarse las denuncias relativas a los hechos y conductas denunciables en sus páginas web. En todo caso, estas autoridades garantizan que la denuncia pueda presentarse tanto de forma escrita como verbal.

Las autoridades que cuentan con canales específicos son las siguientes:

- Autoridad Independiente de Protección del Informante¹
- Banco de España: <https://www.bde.es/wbe/es/para-ciudadano/gestiones/canal-de-denuncias-del-banco-de-espana/>
- Comisión Nacional del Mercado de Valores: <https://www.cnmv.es/portal/whistleblowing/presentacion.aspx>
- Agencia Española de Protección de Datos: <https://www.aepd.es/la-agencia/transparencia/canal-proteccion-informante>

7. Tratamiento de datos de carácter personal

Los datos personales que pueden llegar a tratarse en el curso de un expediente dentro del Procedimiento del Canal de Denuncias serán tratados con la máxima confidencialidad.

¹ Aun no constituida.

La finalidad del tratamiento de datos personales del Canal de Denuncias es la de gestionar la comunicación de una conducta irregular cuando el usuario desee informar sobre sospechas de conductas irregulares, actos ilícitos o incumplimientos normativos. LIFT puede obtener datos directamente del denunciante como de terceros (ej. testigos, investigado, áreas de LIFT, informes periciales o policiales).

Los usuarios del Canal de Denuncias pueden ejercitar sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad, respecto del tratamiento del que es responsable LIFT mediante escrito dirigido a LIFT a la dirección indicada anteriormente acreditando su identidad o bien por correo electrónico a la dirección electrónica: rgpd@auratechlegal.es

8. Aprobación, revisión y publicidad de la política

La presente Política estará disponible en la página web de la Entidad y resultará efectiva y exigible a todas las personas competentes desde su publicación.

La aprobación de la presente Política corresponde al Consejo de Administración de la Entidad, así como las posteriores modificaciones que se produzcan. La Política será actualizada y/o modificada, al menos, en los siguientes casos:

- cuando tengan lugar cambios legales o normativos que afecten a la Política.
- a propuesta 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 a en cada momento.

Sin perjuicio de lo anterior, se llevará a cabo una revisión de la Política, al menos una vez al año, sirviéndose de medios internos o externos.