

01 diciembre 2023, Sant Feliu De Buixalleu

A todos los empleados de RETAL IBERIA, SLU

¡Queridos compañeros!

Nos complace anunciar la adopción del Procedimiento del Sistema Interno de Información (“Procedimiento”), un paso importante para garantizar la transparencia, el cumplimiento y la protección de los denunciantes dentro de RETAL IBERIA, SOCIEDAD LIMITADA Unipersonal (“Empresa”).

El Procedimiento se ha desarrollado tras la adopción de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, sobre la protección de las personas que denuncian infracciones del Derecho de la Unión, por la que se establece un marco unificado y sólido para la protección de denunciantes en todos los estados miembros de la Unión Europea.

El objetivo principal de esta legislación es fomentar la denuncia de malas conductas, corrupción y otras infracciones de la legislación de la UE proporcionando salvaguardias legales contra represalias.

Este documento describe las disposiciones clave del Procedimiento y su funcionamiento.

1. Objetivo: El Procedimiento ha sido establecido de conformidad con la Ley 2/2023, de 20 de febrero, de protección de las personas físicas que denuncian infracciones normativas y de lucha contra la corrupción, por la que se transpone la Directiva (UE) 2019/1937 en España. Describe los principios que rigen el sistema de información interno de la Compañía y las salvaguardias para los denunciantes.

2. Función: La Compañía ha establecido un sistema de información interno designado para recibir y procesar informes sobre ciertas violaciones de las leyes cometidas por la Compañía o cualquiera de su personal a través de canales de información internos, es decir, buzón de correo electrónico especial y personas individuales autorizadas para recibir el informes y procesarlos de forma segura y confidencial.

La Consejera Delegada Ester Masó Donadeu es la responsable de la implantación del Sistema y el Emmanuel Duffaut ha sido nombrado Responsable del Sistema.

3. Ámbito Personal (a quién aplica): El Procedimiento aplica a diversas personas físicas, incluyendo a todos los empleados de la Compañía, trabajadores por cuenta propia, accionistas y aquellos que trabajan bajo contratistas o proveedores. También están cubiertos los voluntarios, pasantes y trabajadores en periodos de formación. Todas aquellas personas y otras personas vinculadas a la empresa disfrutan de las garantías



de protección de su identidad, confidencialidad y secreto de la comunicación, y, como punto más importante, **protección contra represalias** para garantizar que una denuncia de buena fe no se convierta en despido. o cualquier otro trato negativo hacia el reportero.

4. Incumplimientos a Denunciar: Los canales de información internos están designados para recibir denuncias sobre **incumplimientos legales** relacionados con diversas materias, incluido el Derecho de la Unión Europea e infracciones penales o administrativas. El Procedimiento especifica los tipos de incumplimientos que se pueden denunciar.

Un punto a tener en cuenta es que estos canales internos no están designados para recibir inquietudes sobre violaciones de las normas éticas descritas en el Código de Conducta Empresarial del Grupo RETAL y otras políticas de la Compañía. Debido a ciertas razones legales y operativas, incluyendo la

necesidad de obedecer reglas estrictas en el manejo de datos, la Compañía estableció canales locales especiales para procesar estos informes específicos.

Informes recibidos accidentalmente a través de canales inapropiados, p.e. por una secretaria, su director directo o un colega a nivel de grupo, debe remitirse inmediatamente al canal adecuado.

5. Canales de Información: La Sociedad ha establecido los siguientes canales de denuncia, a saber:

Por correo electrónico:

whistleblower@retaliberia.com

Por correo postal:

RETAL IBERIA, SLU
Atención Responsable
del Sistema de
Información Interno.
Ctra Comarcal C-35,
Sector 2, Parcela 5, Sant
Feliu De Buixalleu,
17451 Girona, España

Presencialmente:

Responsable del
Sistema Contactar por
teléfono al +34 650 450
796 dentro del horario
habitual horas para
concertar una cita.

Si un informe afecta al Responsable del Sistema, dicho informe podrá entregarse a la Consejera Delegada Ester Masó Donadeu personalmente o por correo postal al domicilio de la Sociedad, y se tramitará conforme al Procedimiento.

Se insta a todos los colegas a enviar sus inquietudes y denunciar violaciones a la ley en el ámbito del Procedimiento a través de uno de los canales antes mencionados. **¡Los informes pueden ser anónimos!**

6. Confidencialidad: Los denunciadores tienen derecho a mantener su identidad en secreto. El Procedimiento garantiza que se tomen medidas para mantener la confidencialidad de los datos, especialmente la identidad del denunciante.

7. Secreto: La información dentro del sistema permanece confidencial y sólo es accesible al personal autorizado. Se podrán hacer excepciones en cumplimiento de la ley o para investigaciones necesarias.

8. Tratamiento de Datos Personales: El tratamiento de datos personales se ajusta a la normativa aplicable. El acceso a los datos personales es limitado y los datos se conservan sólo durante el tiempo necesario.

9. Prohibición de represalias: Cualquier forma de represalia está expresamente prohibida. Los actos de represalia se tratan como infracciones, se investigan y pueden dar lugar a acciones disciplinarias.

10. Protección de las personas interesadas: Las personas afectadas por un informe, es decir, aquellas acusadas de irregularidades en el mensaje, tienen derecho a ser consideradas inocentes, defenderse y acceder a información relevante mientras su identidad esté protegida.

11. Incumplimiento: El incumplimiento del Procedimiento será investigado y puede dar lugar a responsabilidad disciplinaria o de otro tipo según las leyes aplicables.

Alentamos a cada empleado a familiarizarse con el Procedimiento y contribuir al establecimiento de una cultura de integridad y responsabilidad dentro de la Empresa.

Atentamente,

Olexandr Kachanov
Administrador Único

Ester Masó Donadeu
Directora General

Emmanuel Duffaut
Responsable del Sistema



Aprobado por el Socio Único el 01 de diciembre de 2023

Adoptado por decisión del Administrador Único de fecha 01 de diciembre de 2023

RETAL IBERIA, SOCIEDAD LIMITADA Unipersonal PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES

1. OBJETO DEL DOCUMENTO

- 1.1 El presente documento desarrolla el procedimiento de gestión de informaciones (el "**Procedimiento de Gestión**") adoptado por RETAL IBERIA, SOCIEDAD LIMITADA Unipersonal (la "**Empresa**", la "**Sociedad**" o "**nosotros**").
- 1.2 El Procedimiento de Gestión establece los principios generales del sistema interno de información y de protección de los informantes. El Procedimiento de Gestión sigue 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 (la "**Ley 2/2023**").
- 1.3 Además, el Procedimiento de Gestión describe la forma en la que se procesan las comunicaciones que se reciben a través de nuestros canales internos de información sobre determinadas infracciones de las normas.
- 1.4 El presente Procedimiento de Gestión establece garantías para salvaguardar la independencia, la confidencialidad y la protección de datos de todas las comunicaciones recibidas. Asimismo, cumple con todas las obligaciones exigidas por la Ley 2/2023 relativas al sistema interno de información y los canales internos de información.

2. SISTEMA INTERNO DE INFORMACIÓN COMPOSICIÓN Y CONTROL

- 2.1 El sistema interno de información (el "**Sistema de Información**") comprende los siguientes elementos:
 - (a) el presente Procedimiento de Gestión;
 - (b) los canales internos de información establecidos por la Empresa;
 - (c) los órganos de gobierno y gestión de la Empresa, el responsable del Sistema de Información, sus funciones y responsabilidades tal y como se describen en las respectivas políticas;
 - (d) los manuales, reglamentos y otros documentos adoptados por la Empresa.
- 2.2 El Director General es la persona responsable de la implementación del Sistema de Información.
- 2.3 El Sistema de Información será gestionado por un directivo de la Empresa (el "**Responsable del Sistema**") nombrado por el Administrador Único. El Responsable del Sistema podrá desempeñar esta función junto con el resto de las funciones de su puesto o cargo en la Empresa siempre que no exista conflicto de interés.
- 2.4 Determinadas funciones del Sistema de Información podrán ser delegadas en directivos de la Empresa o en otras personas cuando se den ciertas circunstancias. Entre estas circunstancias

se incluyen los casos en que el Responsable del Sistema no pueda desempeñar temporalmente su función, o los supuestos en que la comunicación de información afecte al Responsable del Sistema o a una persona asociada éste. En cualquier caso, deberán adoptarse las medidas necesarias para asegurar que tales delegaciones se ajustan a los principios y garantías establecidos en el presente Procedimiento de Gestión.

- 2.5 La Sociedad notificará tanto el nombramiento como el cese del Responsable del Sistema a la Autoridad Independiente de Protección del Informante (la "**AAI**"). Además, la Empresa comunicará también a las autoridades u órganos competentes de las Comunidades Autónomas en el ámbito de sus respectivas competencias cuando sea necesario. En ambos casos, la notificación se efectuará en los diez días hábiles siguientes al nombramiento o cese del Responsable del Sistema. Si la notificación se refiere al cese del Responsable del Sistema, será necesario que la notificación vaya acompañada de las razones que han justificado el citado cese.
- 2.6 El Responsable del Sistema desempeñará sus funciones de forma independiente y autónoma respecto del resto de los órganos de la Empresa. Además, no podrá recibir instrucciones de ningún tipo en su ejercicio y deberá disponer de todos los medios personales y materiales necesarios para el desempeño de sus funciones.

3. **ÁMBITO SUBJETIVO**

El Procedimiento de Gestión es de aplicación a las personas tengan conocimiento sobre infracciones en un contexto laboral o profesional (denominadas cualquiera de ellas de forma individual o conjuntamente como el "**Informante**"). El Informante puede ser:

- (a) un empleado;
- (b) un trabajador autónomo;
- (c) accionistas, partícipes, miembros del órgano de administración, dirección o supervisión de la Sociedad, incluidos los miembros no ejecutivos;
- (d) una persona que trabaja para o bajo la supervisión y dirección de contratistas, subcontratistas o proveedores.

La consideración como Informante y la protección de este Procedimiento de Gestión se extiende a:

- (a) voluntarios;
- (b) becarios; y
- (c) trabajadores en periodos de formación, independientemente de que reciban o no remuneración.

Todo lo anterior se aplica a las personas cuya relación laboral ya ha finalizado (cuando la información sobre infracciones se haya obtenido en el marco de una relación laboral o estatutaria) o aún no haya comenzado (cuando la información sobre infracciones se haya obtenido en el proceso de selección o negociación precontractual).

También se consideran Informantes y, por tanto, se encuentran protegidos por la Ley 2/2023, las personas físicas que puedan sufrir represalias y que:

- (a) asistan de cualquier forma al Informante dentro de la Empresa;
- (b) estén relacionados con el Informante como, por ejemplo, compañeros de trabajo o familiares.

La protección del presente Procedimiento de Gestión se extiende además a las personas jurídicas con las que o en las que un Informante:

- (a) es empleado o mantiene cualquier otro tipo de relación laboral; o
- (b) tiene una participación significativa que permite al Informante influir en la entidad jurídica participada.

Asimismo, el Procedimiento de Gestión protege a todas las demás categorías de Informantes protegidos por la Ley 2/2023.

4. CONOCIMIENTO DEL PROCEDIMIENTO DE GESTIÓN

El Procedimiento de Gestión deberá entregarse a los empleados y exponerse en los locales de la Sociedad. Además, estará disponible para todos los empleados de la Sociedad a través de la intranet en el siguiente enlace: <https://retalcorp.sharepoint.com>. Asimismo, el Procedimiento de Gestión podrá ser publicado a través de otras fuentes.

5. INFRACCIONES QUE DEBEN COMUNICARSE

5.1 Los canales internos de información están designados para recibir comunicaciones (la "**Comunicación**" o las "**Comunicaciones**") sobre las siguientes infracciones (denominadas cualquiera de ellas de forma individual o conjuntamente como "**Infracción**"):

a) Cualesquiera acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea siempre que:

1. Entren dentro del ámbito de aplicación de los actos de la Unión Europea enumerados en el anexo de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno, en relación con los siguientes ámbitos:

- contratación pública;
- servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo;
- seguridad y conformidad de los productos;
- seguridad en el transporte;
- protección del medio ambiente;
- protección contra las radiaciones y seguridad nuclear;
- seguridad de los alimentos y los piensos, salud y bienestar de los animales;
- salud pública;
- protección del consumidor;

protección de la intimidad y los datos personales, seguridad de la red y sistemas de información;

2. Afecten a los intereses financieros de la Unión Europea tal y como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE); o

3. Incidan en el mercado interior, tal y como se contempla en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión Europea 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.

b) Acciones u omisiones que 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.

5.2 Los canales internos de información no deben utilizarse para comunicar conflictos interpersonales o que afecten únicamente al Informante y a las personas a las que se refiera la Comunicación. Tampoco es admisible una Comunicación que contenga exclusivamente información pública o que contenga meros rumores. Además, tampoco se admitirán Comunicaciones sobre acciones u omisiones que no estén cubiertas por el ámbito objetivo del Procedimiento de Gestión o que estén fuera del contexto laboral o profesional.

6. CANALES DE INFORMACIÓN

Canales internos de información

6.1 La Empresa ha establecido varios canales internos de información.

Si un Informante tiene motivos razonables para creer que se ha producido o se está produciendo una Infracción que entra en el ámbito de aplicación del presente Procedimiento de Gestión y que la información es cierta en el momento de la Comunicación, incluso sin la totalidad de las pruebas, se anima a dicha persona a que presente sin demora una Comunicación. Esta Comunicación podrá ser anónima si así lo desea el Informante. Dicha Comunicación podrá realizarse por escrito a través de uno de los siguientes medios:

- por correo electrónico a través de: whistleblower@retaliberia.com; o
- por correo postal a la siguiente dirección:
RETAL IBERIA, SLU
A la atención del Responsable del Sistema Interno de Información
Ctra Comarcal C-35, Sector 2, Parcela 5,
Sant Feliu de Buixalleu,
17451 Girona,
España
- en persona;

A petición del Informante, se podrá presentar una Comunicación verbal al Responsable del Sistema a través de una reunión presencial. Las citas para la reunión presencial pueden concertarse a través de cualquiera de los canales internos de información o poniéndose en contacto directamente con el Responsable del Sistema. El Responsable del Sistema deberá organizar la citada reunión presencial en el plazo de siete días a partir de la recepción de la solicitud.

Las Comunicaciones que se refieran al Responsable del Sistema serán recibidas por el Consejero Delegado personalmente, por correo enviado a la dirección de la Empresa o en una reunión presencial.

- 6.2 Cualquier persona que no se encuentre autorizada a recibir Comunicaciones en virtud del Procedimiento de Gestión deberá remitir la información inmediatamente a través de uno de los canales de información designados al Responsable del Sistema. Al realizar el envío, se debe guardar absoluta confidencialidad en relación con su contenido y garantizar la protección de los datos personales. El incumplimiento de esta obligación será investigado y podrá dar lugar a sanciones disciplinarias.

Canales externos de información

- 6.3 Además de los canales internos de información, se podrá informar de cualquier acción u omisión dentro del ámbito de este Procedimiento de Gestión y de la Ley 2/2023 a través de canales externos de información. Además, se permitirá que se realice una Comunicación a través de los canales externos de forma directa o tras haber realizado una Comunicación a través de los canales internos de información. El Anexo 1 contiene una lista de los canales externos de información existentes al momento de la aprobación del presente Procedimiento de Gestión.

7. PROCEDIMIENTO

7.1 Recepción de Comunicaciones

Las Comunicaciones podrán hacerse por escrito a través del formulario creado al efecto o a través de un escrito elaborado por el propio Informante. Las Comunicaciones pueden enviarse por correo postal, electrónico o entregarse en mano a una de las personas autorizadas para recibirlas según el Procedimiento de Gestión.

Las Comunicaciones realizadas a través de una reunión presencial deben documentarse, con el consentimiento previo del Informante, de una de las siguientes maneras:

- mediante una grabación de la conversación en un formato seguro, duradero y accesible;
- o
- mediante una transcripción completa y exacta de la conversación realizada por el Responsable del Sistema, ofreciendo al Informante la posibilidad de verificar, rectificar y aceptar la transcripción de la conversación mediante su firma.

Se informará al Informante de que sus datos serán tratados según lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 11 de la Ley Orgánica 3/2018, de 5 de diciembre.

7.2 **Registro de las Comunicaciones**

Todas las Comunicaciones recibidas deben registrarse oportunamente en un libro-registro elaborado conforme al Procedimiento de Gestión.

7.3 **Evaluación de las Comunicaciones**

7.3.1 Si la Comunicación se encuentra cumplimentada correctamente y se considera pertinente, se evaluará en un plazo razonable desde su recepción. Si la información no fuera suficiente para valorar la Comunicación, se podrá pedir más información al Informante.

7.3.2 Tras una cuidadosa evaluación, se tomará una de las siguientes decisiones:

- i. inadmitir la Comunicación sin que se efectúe una investigación de la misma. Esta decisión se podrá tomar siempre que:
 - a) los hechos denunciados no presenten un mínimo de verosimilitud;
 - b) los hechos denunciados no constituyan una infracción contemplada en el Procedimiento de Gestión;
 - c) la Comunicación resulte manifiestamente infundada, o existan indicios racionales de que la información se ha obtenido mediante la comisión de un delito;
 - d) la Comunicación no contenga información nueva o significativa sobre una Infracción habiendo sido objeto de una Comunicación anterior ya concluida.
- ii. adoptar o solicitar la adopción de una o varias medidas cautelares;
- iii. iniciar una investigación de la Comunicación;
- iv. remitir la información a un procedimiento diferente; y/o
- v. recomendar a la dirección de la Empresa que informe a las autoridades policiales, judiciales o administrativas según corresponda.

Toda Infracción que constituya una infracción administrativa debe comunicarse a las autoridades competentes a estos efectos. Cuando los hechos puedan ser indiciariamente constitutivos de delito, la información deberá remitirse inmediatamente al Ministerio Fiscal. Cuando los hechos denunciados afecten a los intereses financieros de la Unión Europea, la información deberá remitirse a la Fiscalía Europea.

La comunicación a las autoridades se realizará siempre que no vulnere la legalidad o los derechos fundamentales de las personas físicas y/o jurídicas que puedan verse afectadas por los hechos en cuestión.

7.4 **Acuse de recibo**

El Responsable del Sistema acusará recibo de la Comunicación al Informante por escrito en un plazo de siete días naturales a partir de su recepción, salvo que ello pueda poner en peligro la confidencialidad de la Comunicación. En concreto, no se enviará acuse de recibo cuando el envío revele la identidad del Informante, el Informante no haya facilitado su dirección en la Comunicación, la Comunicación sea anónima o el Informante haya pedido expresamente que no se le informe de la recepción de la Comunicación.

7.5 **Investigación de las Comunicaciones**

7.5.1 Nos esforzaremos por investigar todas las Comunicaciones admisibles.

- 7.5.2 El Responsable del Sistema designará a un instructor competente e imparcial. Si la Comunicación afecta al Responsable del Sistema, el instructor será nombrado por otro miembro de la dirección de la Empresa que no se encuentre en conflicto de interés.
- 7.5.3 Los instructores no deben tener ningún interés personal en el resultado de la investigación. Cualquier instructor que tenga un interés personal en el resultado de la investigación deberá abstenerse de participar en la misma y deberá informar de ello por escrito a la persona que autorizó la investigación tan pronto como tenga conocimiento de su interés.
- 7.5.4 En cualquier investigación, se debe respetar el procedimiento regulado, evaluando los hechos en su complejidad y tratando de determinar tanto las Infracciones que entran en el ámbito objetivo del Procedimiento de Gestión como las personas responsables de las mismas. También se debe identificar a quienes ayudaron o se beneficiaron de las Infracciones cometidas.
- 7.5.5 El instructor podrá acceder a documentos e información de la Empresa, visitar los locales y reunirse con los empleados (también de forma confidencial).
- 7.5.6 Toda investigación de una Comunicación dará lugar a un informe escrito que será puesto en conocimiento de la persona que autorizó la investigación.
- 7.5.7 El plazo máximo de investigación de las Comunicaciones no podrá exceder los tres meses. Este plazo comenzará con el acuse de recibo de la Comunicación, si se ha efectuado, o con la expiración del plazo de siete días que se puede efectuar el acuse de recibo. En casos de especial complejidad, el periodo de tres meses puede ampliarse hasta un máximo de otros tres meses adicionales.
- 7.6 **Resultado de la investigación**
- 7.6.1 Cuando, tras la investigación, se detecte la comisión de una Infracción, la Empresa deberá:
- adoptar las medidas adecuadas para resolver la Infracción,
 - imponer las sanciones adecuadas a la persona o personas implicadas; y/o
 - remitir la información a las autoridades competentes, cuando proceda.
- 7.6.2 Las infracciones pueden justificar la adopción de medidas disciplinarias contra la persona afectada. Dichas medidas deberán ajustarse a las leyes, reglamentos y políticas de la Empresa.
- 7.6.3 Las personas que realicen Comunicaciones falsas también podrán ser sancionadas disciplinariamente.
- 7.7. **Comunicación al Informante sobre las medidas adoptadas y/o el seguimiento**
- En la medida en que sea necesario, podrá facilitarse al Informante información sobre las medidas previstas o adoptadas así como el seguimiento y los motivos de dicho seguimiento.
8. **CONFIDENCIALIDAD**
- 8.1 Toda persona que presente una Comunicación tiene derecho a que no se revele su identidad a terceros. Salvo obligación legal o consentimiento explícito, la Empresa no revelará la identidad del Informante o de una persona afectada a nadie que no necesite conocerla.
- 8.2 Para proteger la identidad de las personas afectadas por la Comunicación, se tomarán todas las medidas necesarias para mantener la confidencialidad de sus datos, especialmente del

Informante, cuya identidad sólo podrá ser comunicada a la autoridad judicial, al Ministerio Fiscal o a la autoridad competente en una investigación penal, disciplinaria o sancionadora.

8.3 En ningún caso deberá informarse a la persona afectada de la identidad del Informante.

9. SEGURIDAD

9.1 Toda la información documentada del Sistema de Información será confidencial incluyendo el contenido del informe tras la investigación, los detalles de la recepción de la Comunicación, el acuse de recibo, la evaluación, la investigación, la conclusión y cualquier otro tipo de comentario. Solo en los casos en los que sea estrictamente necesario se compartirá esta información ya sea para la investigación, la acción disciplinaria o el cumplimiento de la ley.

9.2 Sólo el personal autorizado puede acceder al Sistema de Información. En casos excepcionales, podrá compartirse con terceros en cumplimiento de las leyes y siempre que se tomen las medidas adecuadas.

10. TRATAMIENTO DE DATOS PERSONALES

10.1 El tratamiento de datos personales en virtud del Procedimiento de Gestión debe realizarse de conformidad con los principios y normas previstos en las leyes y reglamentos de protección de datos personales aplicables a la Empresa. El Anexo 2 contiene información sobre la protección de datos personales y el ejercicio de derechos.

10.2 En ningún caso serán objeto de tratamiento aquellos datos personales que no sean necesarios para el conocimiento o la investigación de la Comunicación. En su caso, deberán ser inmediatamente suprimidos. Asimismo, deberán suprimirse todos los datos de carácter personal que se refieran a conductas no incluidas en el ámbito de aplicación de la Ley 2/2023.

10.3 La información recibida puede contener una de las categorías especiales de datos personales recogidas en la normativa. Cuando este hecho suceda, dicha información debe suprimirse inmediatamente sin que se proceda a su registro o tratamiento.

10.4 Si se demuestra que la información facilitada o parte de ella es falsa, deberá suprimirse inmediatamente en cuanto se tenga conocimiento de tal circunstancia. Esta premisa no se aplicará cuando dicha falta de veracidad pueda ser constitutiva de delito. En este caso, se conservará la información durante el tiempo que sea necesario para el desarrollo del procedimiento judicial.

10.5 El acceso a los datos personales contenidos en el Sistema de Información debe limitarse exclusivamente a:

- a) El Responsable del Sistema y quien lo gestionen directamente;
- b) una persona responsable de recursos humanos o un organismo competente debidamente designado sólo cuando puedan adoptarse medidas disciplinarias contra un empleado;
- c) una persona responsable de las cuestiones legales en la Empresa, si procede la adopción de medidas legales en relación con los hechos denunciados en la Comunicación;

- d) las personas encargadas del tratamiento de datos personales que se designen en cada momento; o
 - e) el responsable de la protección de datos.
- 10.6 El tratamiento de datos personales por otras personas o su comunicación a terceros es lícito cuando sea necesario para adoptar una medida correctora en la Empresa o desarrollar oportuno procedimiento disciplinario o penal.
- 10.7 Los datos objeto de tratamiento sólo podrán conservarse en el Sistema de Información durante el tiempo necesario para decidir si se inicia una investigación sobre los hechos denunciados.
- 10.8 Transcurridos tres meses desde la recepción de una Comunicación sin investigación, los datos personales recibidos deberán suprimirse, salvo que sean necesarios para el funcionamiento del Sistema de Información. Las Comunicaciones que no se hayan tramitado sólo podrán registrarse de forma anonimizada.
- 10.9 Los empleados y terceros deben ser notificados del tratamiento de datos personales dentro del Sistema de Información. La notificación debe incluir información en este sentido y debe hacerse en una forma que sea igual o sustancialmente similar a la incluida en el Procedimiento de Gestión.

11. PROHIBICIÓN DE REPRESALIAS

- 11.1 Prohibimos expresamente cualquier forma de represalia. Esto incluye cualquier acto u omisión que no esté permitido por la ley o que, directa o indirectamente, implique un trato desfavorable que coloque a las personas que lo sufren en una situación de especial desventaja con respecto a otra en el contexto laboral o profesional únicamente por su condición de Informantes o por haber realizado una revelación pública de información.
- 11.2 Tratamos las represalias como una infracción en sí misma. La Empresa se esfuerza por investigar debidamente todos los actos de represalia. El autor de una represalia puede enfrentarse a una sanción disciplinaria u otra medida apropiada, según exija la ley.
- 11.3 Todo Informante que sufra una represalia debe informar a través de cualquiera de los canales de información internos.

12. PROTECCIÓN DE LAS PERSONAS AFECTADAS

Las personas afectadas por una Comunicación ("**personas afectadas**") tienen derecho a la presunción de inocencia. También tienen derecho de defensa y a acceder al expediente conforme a la ley. Se protegerá su identidad y se mantendrá la confidencialidad de los hechos y datos.

13. CONSERVACIÓN DE REGISTROS

- 13.1. Los informes recibidos y la información pertinente, incluidos los resultados de la evaluación y la investigación, deben consignarse en un registro ("**Libro-Registro**").
- 13.2. El Libro-Registro no debe ser público. Sólo podrá divulgarse a petición motivada de la autoridad judicial competente, mediante auto, dentro del procedimiento judicial y bajo su control.
- 13.3. Los informes y la documentación correspondiente, incluidos los datos personales que contengan, deberán conservarse en un formato seguro, duradero y accesible. Sólo deben conservarse durante el tiempo necesario para tramitar el informe que finaliza la investigación de la Información y, en cualquier caso, durante un máximo de cinco años a partir de la fecha en que finalice el procedimiento de comunicación. Esto no se aplica cuando la ley o un procedimiento judicial exijan un plazo más largo.

14. INCUMPLIMIENTO

El incumplimiento del Procedimiento de Gestión debe ser investigado y puede dar lugar a responsabilidad disciplinaria y/o de otro tipo según la legislación aplicable.

RETAL IBERIA, SOCIEDAD LIMITADA Unipersonal
PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES

Anexo 1

Lista de canales externos de información

- (i) Oficina Europea de Lucha contra el Fraude (OLAF) (https://fns.olaf.europa.eu/main_es.htm)
- (ii) Banco de España (<https://www.bde.es/wbe/es/para-ciudadano/gestiones/canal-de-denuncias-del-banco-de-espana/>)
- (iii) Comisión Nacional de los Mercados y la Competencia (CNMC) (<https://edi.cnmc.es/buzones-anonimos/sica>)
- (iv) Comisión Nacional del Mercado de Valores (CNMV) (<https://www.cnmv.es/portal/whistleblowing/presentacion.aspx#:~:text=Escribiendo%20a%3A%20Comunicaci%C3%B3n%20de%20Infracciones,revelar%20su%20identidad%20o%20no>)
- (v) Canal del Servicio Nacional de Coordinación Antifraude (<https://www.igae.pap.hacienda.gob.es/sitios/igae/esES/snca/Paginas/ComunicacionSNCA.aspx>).
- (vi) Buzón antifraude - Canal de denuncias del Mecanismo para la Recuperación y Resiliencia (<https://planderecuperacion.gob.es/buzon-antifraude-canal-de-denuncias-del-mecanismo-para-la-recuperacion-y-resiliencia>).
- (vii) Oficina Antifraude de Cataluña (<https://seuelectronica.antifrau.cat/es/denuncia.html>).
- (viii) Oficina Andaluza Antifraude (<https://buzon.antifraudeandalucia.es/#/>).
- (ix) Canal de denuncias del portal de transparencia y gobierno abierto de la Xunta de Galicia (https://transparencia.xunta.gal/canle-de-denuncias?langId=es_ES).
- (x) Oficina de atención a la ciudadanía de Cantabria ([https://www.federcantabria.es/prevencion-del-riesgo-de-fraude#:~:text=Canales%20de%20denuncia&text=Por%20Internet%20a%20trav%C3%A9s%20buz%C3%B3n,\(desde%20fuera%20de%20Cantabria\)](https://www.federcantabria.es/prevencion-del-riesgo-de-fraude#:~:text=Canales%20de%20denuncia&text=Por%20Internet%20a%20trav%C3%A9s%20buz%C3%B3n,(desde%20fuera%20de%20Cantabria))).
- (xi) Canal de denuncias del Gobierno de Aragón (<https://www.aragon.es/-/next-generation-eu-antifraude#anchor4>).
- (xii) Canal de lucha contra la corrupción del Principado de Asturias (https://transparencia.asturias.es/detalle/-/categories/1035112?p_r_p_categoryId=1035112&com_liferay_asset_categories_navigation_web_portlet_AssetCategoriesNavigationPortlet_articleId=2627345&articleId=2627345&title=Canal%20de%20lucha%20contra%20la%20corrupci%C3%B3n&redirect=https%3A%2F%2Ftr)

ansparencia.asturias.es%2Fgeneral%2F-%2Fcategories%2F1035112%3Fp_r_p_categoryId%3D1035112).

- (xiii) Oficina de Prevención y Lucha contra la Corrupción en las Illes Balears (<https://www.oaib.es/denuncias/>).
- (xiv) Oficina Municipal contra el Fraude y la Corrupción de Madrid (<https://www.madrid.es/portales/munimadrid/es/Inicio/EI-Ayuntamiento/Denuncias/?vgnextfmt=default&vgnextoid=789a088847b26810VgnVCM200001f4a900aRCRD&vgnnextchannel=ce069e242ab26010VgnVCM100000dc0ca8c0RCRD&idCapiitulo=11922007&rm=00369bbb53158610VgnVCM1000001d4a900aRCRD>).
- (xv) Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana (<https://www.antifraucv.es/buzon-de-denuncias-2/>).
- (xvi) Oficina de Buenas Prácticas y Anticorrupción de la Comunidad Foral de Navarra (OANA) (<https://oana.es/es/denuncia>)

RETAL IBERIA, SOCIEDAD LIMITADA Unipersonal
PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES

Anexo 2

Información sobre la protección de datos personales y el ejercicio de derechos

Información a la que se refiere el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (el "**Reglamento (UE) 2016/679**"), y 11 de la Ley Orgánica 3/2018, de 5 de diciembre.

La identidad y los datos de contacto del responsable del tratamiento y, en su caso, de su representante:	RETAL IBERIA, SOCIEDAD LIMITADA Unipersonal Ctra Comarcal C-35, Sector 2, Parcela 5, Sant Feliu De Buixalleu, 17451 Girona, España. Tel.+34972865730; correo electrónico: iberia@retalgroup.com
Los datos de contacto del responsable de la protección de datos, si procede:	No se aplica.
Los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento:	Finalidad del tratamiento: recogida y tratamiento de información sobre infracciones. Base jurídica del tratamiento: Artículos 6.1. (a), (c), (e) del Reglamento (UE) 2016/679, 8 de la Ley Orgánica 3/2018, de 5 de diciembre, y 11 de la Ley Orgánica 7/2021, de 26 de mayo.
Cuando el tratamiento se base en el artículo 6, apartado 1, letra f), del Reglamento (UE) 2016/679, los intereses legítimos perseguidos por el responsable del tratamiento o por un tercero:	No se aplica.
Los destinatarios o categorías de destinatarios de los datos personales, en su caso:	Los responsables del tratamiento, la autoridad pública, la agencia u otro organismo al que se comuniquen los datos personales con arreglo a la legislación aplicable, las personas encargadas de la investigación de las Comunicaciones y de la aplicación de las medidas respectivas.
El hecho de que el responsable del tratamiento tenga la intención de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o en el caso de las	Los datos personales podrán transferirse a un tercer país -miembro de la Unión Europea, Gran Bretaña u otro país u organización internacional- siempre que dicha transferencia

<p>transferencias a que se refieren los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, Reglamento (UE) 2016/679 referencia a las garantías apropiadas o adecuadas y los medios para obtener una copia de las mismas o dónde se han puesto a disposición:</p>	<p>cumpla las disposiciones del Reglamento (UE) 2016/679.</p>
<p>El periodo durante el cual se almacenarán los datos personales o, si no es posible, los criterios utilizados para determinar dicho periodo:</p>	<p>Los datos se conservarán durante el tiempo necesario para el cumplimiento de lo dispuesto 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. Los datos no podrán conservarse por un periodo superior a cinco años.</p>
<p>La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse a su tratamiento, así como el derecho a la portabilidad de los datos:</p>	<p>Usted tiene derecho a solicitar al responsable del tratamiento el acceso a los datos personales y su rectificación o supresión. También tiene derecho a la limitación de su tratamiento, o a oponerse a su tratamiento, así como el derecho a la portabilidad de los datos.</p>
<p>Cuando el tratamiento se base en el artículo 6, apartado 1, letra a), o en el artículo 9, apartado 2, letra a), del Reglamento (UE) 2016/679, la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento antes de su retirada:</p>	<p>En la medida de los datos tratados con arreglo al artículo 6, apartado 1, letra a), o al artículo 9, apartado 2, letra a), del Reglamento (UE) 2016/679, usted tiene derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento antes de su retirada.</p>
<p>Derecho a presentar una reclamación ante una autoridad de control:</p>	<p>Tiene derecho a presentar una reclamación ante una autoridad de control:</p> <p>Agencia Española de Protección de Datos C/Jorge Juan, 6 28001 Madrid España Tel. +34 900 293 183 https://sedeagpd.gob.es/</p>
<p>Si el suministro de datos personales es un requisito legal o contractual, o un requisito necesario para celebrar un contrato, así como si el interesado está obligado a proporcionar los datos personales y de las posibles consecuencias de no hacerlo:</p>	<p>El suministro de datos personales no es un requisito legal o contractual ni un requisito necesario para celebrar un contrato. Usted no está obligado a facilitar los datos personales. Las posibles consecuencias de no facilitar dichos datos pueden obstaculizar la correcta evaluación de su Comunicación, la debida</p>

	investigación y la adopción de las medidas oportunas.
La existencia de la toma de decisiones automatizada, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, del Reglamento (UE) 2016/679 y, al menos en esos casos, información significativa sobre la lógica implicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado:	La toma de decisiones automatizada no existe.
La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679:	Usted tiene los derechos de acceso a la rectificación, supresión, limitación del tratamiento, oposición y toma de decisiones individuales automatizadas así como el derecho a no ser objeto de una decisión basada únicamente en un tratamiento automatizado ejercitables según lo establecido en el Reglamento (UE) 2016/679.