Política y procedimiento del sistema interno de información de Tubasys, S.L.U.

1. Objeto

El presente documento se establece con objeto de diseñar, establecer y gestionar de forma segura el Sistema Interno de Información de TUBASYS, S.L.U., garantizando la confidencialidad de la identidad del informante y de cualquier tercero mencionado. Asimismo, incluye las actuaciones necesarias para su gestión y tramitación, así como la protección de datos, impidiendo el acceso a personal no autorizado.

Este procedimiento ha sido desarrollado según 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.

2. Ámbito De Aplicación

2.1. Ámbito De Aplicación Personal

El presente sistema se aplicará a aquellas personas que hayan obtenido información sobre infracciones en un contexto laboral o profesional, comprendiendo en todo caso:

a) las personas que tengan la condición de trabajadores por cuenta ajena;

b) los autónomos;

c) los accionistas, partícipes y personas pertenecientes al órgano de administración, alta dirección o supervisión de la empresa, incluidos los miembros no ejecutivos;

d) cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

También se aplicará a las personas informantes que comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral o estatutaria ya finalizada, personas voluntarias, becarias, personal en periodos de formación con independencia de que perciban o no una remuneración, así como a aquellas personas cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.

Las medidas de protección de la persona informante también se aplicarán, en su caso, a quienes ejerzan la representación legal de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo a la persona informante.

Estas medidas de protección a la persona informante también se aplicarán a:

a) personas físicas que, en el marco de la organización en la que preste servicios la persona informante, asistan al mismo en el proceso,

b) personas físicas que estén relacionadas con la persona informante y que puedan sufrir represalias, como compañeros/as de trabajo o familiares de la persona informante, y

c) 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.

2.2. Ámbito De Aplicación Material

El presente procedimiento establece normas mínimas comunes para la protección de las personas que informen sobre:

a) Infracciones del Derecho de la Unión:

1) infracciones que entren dentro del ámbito de aplicación de los actos de la Unión 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, relativas a los ámbitos siguientes:

- contratación pública,
- servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo,
- seguridad de los productos y conformidad,
- seguridad del transporte,
- protección del medio ambiente,
- protección frente a las radiaciones y seguridad nuclear,

- seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales,
- salud pública,
- protección de las personas consumidoras,
- protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información;

2) infracciones que afecten a los intereses financieros de la Unión tal como se contemplan en el artículo 325 del TFUE y tal como se concretan en las correspondientes medidas de la Unión;

3) infracciones relativas al mercado interior, tal como se contemplan en el artículo 26, apartado 2, del TFUE, incluidas las infracciones de las normas de la Unión 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 a prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable del 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 todas aquellas infracciones penales o administrativas graves o muy graves que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.

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.

EXCLUSIONES:

- Informaciones que afecten a la información clasificada.
- Tampoco afectará a las obligaciones que resultan de la protección del secreto profesional de los profesionales de la medicina y de la abogacía, del deber de

confidencialidad de las Fuerzas y Cuerpos de Seguridad en el ámbito de sus actuaciones, así como del secreto de las deliberaciones judiciales.

- 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.

3. Responsabilidades

ÓRGANO DE ADMINISTRACIÓN

- Implantar el Sistema interno de información, previa consulta con la representación legal de las personas trabajadoras.
- Tendrá la condición de responsable del tratamiento de los datos personales de conformidad con lo dispuesto en la normativa sobre protección de datos personales.
- Designación, destitución y/o, cese de los miembros del Sistema Interno de Información.
- Definir y aprobar la Política o Estrategia que define los principios básicos del Sistema Interno de información.
- Aprobación del procedimiento de gestión de informaciones del Sistema Interno de Información, definido en el presente documento.

RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN

- Recibir, gestionar e investigar las informaciones recibidas por el canal formal del sistema interno de información, haciendo un seguimiento con la máxima diligencia.
- Desarrollar sus funciones de forma independiente y autónoma respeto del resto de órganos de la entidad, disponiendo de medios materiales y personales necesarios para llevarlas a cabo.
- Mantener comunicación con la persona informante.
- Proporcionar respuesta.

- Cumplir con las disposiciones sobre protección de datos personales.
- Garantizar la confidencialidad del informante y de la persona afectada por la información.
- Respetar la presunción de inocencia y al honor de las personas afectadas.
- Informar a las personas afectadas de las acciones u omisiones que se le atribuyen, así como mantener comunicación con el afectado en tiempo y forma para garantizar la investigación.
- Prohibir las represalias a las personas informantes, así como amenazas y/o tentativas de represalias, y asegurar que se toman las medidas necesarias para prevenirlas.

RESTO DE PERSONAL

- Derivar en el Responsable del Sistema de Información cualquier comunicación que reciban en relación con esta materia.
- Garantizar la confidencialidad de la información recibida y comunicada al Responsable del Sistema Interno de Información.

4. Desarrollo

Las personas que trabajan para una organización o están en contacto con ella en el contexto de sus actividades laborales o profesionales son a menudo las primeras en tener conocimiento de amenazas o perjuicios para el interés público que surgen en ese contexto. Al informar sobre infracciones dichas personas actúan como informantes y por ello desempeñan un papel clave a la hora de descubrir y prevenir esas infracciones y de proteger el bienestar de la sociedad. Sin embargo, las personas informantes potenciales suelen renunciar a informar sobre sus preocupaciones o sospechas por temor a represalias. Debido a esto, y considerando además que la protección de las personas informantes es necesaria para mejorar la aplicación del derecho en materia de contratación pública, en cumplimiento de la normativa legal, TUBASYS, S.L.U. establece un Sistema de Interno de Información, que canalizará formalmente las posibles comunicaciones sobre infracciones penales o administrativas (graves o muy graves) que ocurran en la Organización.

Por ello se ha diseñado, establecido y gestionado un sistema que funciona de forma segura y que garantiza la confidencialidad de la identidad de la persona informante y de cualquier

tercera persona incluida en la información facilitada, otorgando protección adecuada frente a posibles represalias.

4.1. Responsable Del Sistema Interno De Información

El Órgano de Administración u Órgano de Gobierno será el competente para la designación de las personas físicas responsables de la gestión de dicho sistema o «Responsables del Sistema Interno de Información», y de su destitución o cese. Deberá ser personal directivo de la Empresa, que ejercerá su cargo con independencia del Órgano de Administración o de Gobierno.

El Responsable del Sistema de Información es un órgano colegiado, y se debe delegar en uno de sus miembros las facultades de gestión del Sistema interno de información y de tramitación de expedientes de investigación.

Tanto el nombramiento como el cese de las personas integrantes del órgano colegiado serán notificadas a la Autoridad Independiente de Protección del Informante, A.A.I., o, en su caso, a las autoridades u órganos competentes de las comunidades autónomas, en el ámbito de sus respectivas competencias, en el plazo de los diez días hábiles siguientes a su creación, especificando, en el caso de su cese, las razones que han justificado dicho nombramiento.

Dichas personas desarrollarán sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad. No podrán recibir instrucciones de ningún tipo en su ejercicio, y deberán disponer de todos los medios personales y materiales necesarios para llevarlas a cabo.

4.2. Procedimiento De Gestión De Informaciones

4.2.1. Política General del Sistema Interno de Información

TUBASYS, S.L.U. ha definido una política o estrategia que incluye los principios básicos generales del Sistema interno de información y defensa de la persona informante. Esta política ha sido comunicada en el seno de la Empresa.

4.2.2. Canales internos

Las informaciones deben hacerse llegar por el canal interno establecido, siendo este:

- Plataforma web: https://taleso.es/es/tubasys/

Se garantiza la confidencialidad de la persona informante en todo momento. La aplicación requiere la inclusión de una dirección de correo electrónico que quedará almacenada de manera cifrada en la propia plataforma, de modo que no será accesible bajo ningún concepto a las personas Responsables del Sistema Interno de Información, garantizándose el anonimato de la persona informante.

En cualquier caso, los canales habilitados han de ser debidamente publicitados en el seno de la Empresa para que cualquier persona incluida en el ámbito de aplicación del presente documento pueda informar de posibles infracciones.

4.2.3. Gestión de informaciones

El Sistema Interno de Información debe garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la Empresa, con el fin de que ésta sea la primera en tener conocimiento de la posible irregularidad. Para ello, el Sistema Interno de Información se gestionará de TUBASYS, S.L.U. del siguiente modo:

- ENVÍO DE INFORMACIÓN: Para realizar una comunicación, la persona informante deberá acceder al apartado de la web de la empresa denominado "Canal Ético". Una vez se acceda, se abrirá un banner con la información básica de protección de datos personales en primera capa, con un link habilitado de acceso a la segunda capa de información. Se deberá aceptar que se ha leído y entendido la Política de Privacidad y darle a "continuar".

Una vez hecho lo anterior, se le redireccionará a la web https://taleso.es/es/tubasys/, donde deberá acudir al apartado "crear nuevo informe". En caso de querer realizar una comunicación de manera anónima, se deberá seleccionar la opción "Deseo informar de manera anónima" y cumplimentar los campos obligatorios (empresa relacionada con la información vertida y dirección de correo electrónico).

Será siempre obligatorio el campo "Declaro que todo lo anterior es cierto", a fin de evitar la comunicación de informaciones falsas. La comprobación de informaciones manifiestamente falsas podrán ser objeto de las sanciones establecidas en el Convenio Colectivo.

Una vez finalizado se deberá seleccionar "Enviar el Formulario". En ese momento, se recibirá un correo electrónico con el número de identificador de la información comunicada para su posterior seguimiento en el apartado "Seguimiento de Informe" del panel principal de la aplicación.

El correo electrónico que se incluya en el formulario quedará encriptado en la propia aplicación, de modo que no será posible conocer la identidad de la persona informante. Su recogida se realiza a efectos de poder enviarle un código identificador para la realización del seguimiento a través de la plataforma y poder enviarle correos electrónicos conforme se dé respuesta a la información comunicada.

- ACUSE DE RECIBO: una vez recibida la información a través de la plataforma, esta enviará un acuse de recibo a la persona informante de manera instantánea (plazo máximo de 7 días desde la recepción de ésta) consistente en un número identificador con el que poder hacer seguimiento de la información comunicada.

- RECEPCIÓN INFORMACIÓN: Todas las informaciones serán comunicadas y gestionadas por el canal interno https://taleso.es/es/tubasys/

Siempre que se trate de una persona informante identificada (no anónimo), al hacer la comunicación, ésta podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones.

Las comunicaciones también podrán ser realizadas de manera anónima, siendo gestionadas y tramitadas como cualquier otra información recibida a través del Sistema Interno de Información.

De todas formas, en la aplicación constará toda la información necesaria para la investigación disponiéndose de total trazabilidad en el sistema. Las personas informantes siempre podrán acudir a la aplicación para ver el estado de tramitación y comunicarse con las personas Responsables del Sistema.

En caso de recibirse informaciones no incluidas en el objeto del presente procedimiento, dichas comunicaciones y sus remitentes quedarán fuera del ámbito de protección dispensado por el sistema, derivando el contenido de la información a las personas responsables de su gestión.

Todas las informaciones serán gestionadas por una empresa distinta de la nuestra, con la que se ha firmado el correspondiente contrato de prestación de servicios y encargado de tratamiento, con la finalidad de dotar de una mayor garantía de cumplimiento al sistema implantado.

- TRAMITACIÓN / INVESTIGACIÓN: Una vez se reciba la información en la plataforma y, emitido de manera automática el acuse de recibo, las personas Responsables del Sistema

Interno de Información iniciarán su investigación dejando constancia de ésta en el Sistema Interno de Información, el cual comprenderá los siguientes ítems:

a. N.º de Registro.

b. Fecha de entrada.

c. Persona informante: Este campo se completará con el nombre y apellidos de la persona informante y, en caso de tratarse de una persona que no pertenezca a la empresa se indicará la empresa a la que pertenece. En caso de que la información recibida sea anónima se indicará el término "anónima".

d. Descripción de los hechos: Se incluirá un breve extracto de la información recibida.

e. Investigación: La investigación incluirá consultas internas y con asesores jurídicos externos; entrevistas a las personas afectadas, a la persona informante y/o a cualquier otra que pudiera resultar implicada; solicitud de antecedentes y aclaraciones, así como cualquier otra prueba documental.

f. Sospechas de mala fe.

g. Conclusiones y acciones tomadas.

h. Verificación de la información.

i. Fecha de respuesta a la persona informante (máximo 3 meses prorrogable por 3 meses más en caso de expediente de gran complejidad).

j. Puesta en conocimiento de la Autoridad Competente y fecha (si se da el caso).

k. Sanciones disciplinarias.

l. Fecha de cierre.

Se dispone de un plazo máximo de respuesta de tres meses, a partir del envío del acuse de recibo. En el caso de expedientes de especial complejidad, se podrá posponer el plazo máximo hasta 3 meses más.

Durante la investigación, las personas Responsables del Sistema Interno de información, podrán mantener comunicación con la persona informante para solicitar información adicional tanto si se ha identificado como si no, a través de la plataforma.

La persona afectada por la información será informada de las acciones u omisiones que se le atribuyen y será oída en cualquier momento. Dicha información se facilitará en el momento que se considere más adecuado para no entorpecer la investigación.

Durante todo el proceso y hasta la finalización de la investigación se debe de mantener la presunción de inocencia y respetar el honor de las personas afectadas, así como respetar las disposiciones en materia de protección de datos.

En cualquier momento del proceso, se deberá informar al Ministerio Fiscal de manera inmediata cuando se disponga de indicios de que se haya podido producir la comisión de un hecho delictivo.

- RESOLUCIÓN: Una vez se haya finalizado la investigación se entregará informe a la persona informante y a las personas sobre quienes se esté informando, donde se incluirán las conclusiones a las que hayan llegado las personas que formen parte del Responsable del Sistema Interno de Información, así como las acciones disciplinarias que se llevarán a cabo, en su caso.

- REGISTRO: La información recibida y su investigación se archivarán en la plataforma. Este registro no será público y únicamente se entregará a la Autoridad Judicial previa petición razonada, mediante auto y bajo su tutela.

El plazo de conservación será el que corresponda a la prescripción de cada delito y, en todo caso, por un plazo mínimo de 5 años y máximo de 10 años. Los datos personales de las informaciones serán tratados según se indica en el apartado correspondiente del presente procedimiento.

4.2.4. Revelación Pública

Cuando una persona pone a disposición del público la información sobre acciones y omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave, dispondrá de protección siempre y cuando:

- Haya realizado la comunicación a través de canales internos o externos y no se hayan tomado medidas apropiadas al respecto.

- Tenga motivos razonables para pensar que la infracción puede constituir un peligro inminente o manifiesto para el interés público o existe un riesgo de daños irreversibles, incluido un peligro para la integridad física de una persona, exista riesgo de represalias o

pocas probabilidades de que se lleve a cabo un tratamiento efectivo de la información, mediante la ocultación o destrucción de pruebas.

4.3. Preservación De La Identidad De La Persona Informante Y De Las Personas Afectadas

Las personas Responsables del Sistema Interno de Información, se asegurarán de que se preserve tanto el anonimato y confidencialidad de la persona informante como la de cualquier tercera persona que se mencione. En caso de revelación pública, se garantizará que no se facilite en ningún momento información que permita la identificación de la persona informante, de terceras personas que se mencionen o de las personas afectadas.

Únicamente se facilitará la identidad de la persona informante a la Autoridad Judicial, al Ministerio Fiscal o la Autoridad Administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora, teniendo que comunicar a la persona informante, previamente, que su identidad va a ser revelada, salvo que esta comunicación pueda comprometer la investigación o el procedimiento judicial.

Durante el proceso de investigación, y cuando se comuniquen a las personas afectadas las informaciones recibidas, no se podrá, en ningún caso, informar sobre la identidad de la persona informante o de quien haya llevado a cabo la revelación pública.

4.4. Medidas Para La Protección De Las Personas Afectadas

Durante la tramitación del expediente, las personas afectadas por la comunicación tendrán derecho a la presunción de inocencia, al derecho de defensa y al derecho de acceso al expediente, así como a la misma protección establecida para los informantes, preservándole su identidad y garantizándose la confidencialidad de los hechos y datos del expediente.

4.5. Protección De Datos Personales

4.5.1. Datos personales

Todos los datos personales necesarios para la aplicación del presente procedimiento serán considerados lícitos debiendo ser tratados respetando la normativa en esta materia. Se consideran datos personales los relativos a la persona informante, así como datos de terceras personas, cuando resulte necesarios para la adopción de medidas correctoras o la tramitación de expediente.

No se recopilarán datos de personas que no resulten necesarios para la información y posterior investigación. En caso de recopilar datos de manera accidental, éstos serán eliminados del expediente en cuanto se determine su improcedencia. Del mismo modo, serán tratados los datos de informaciones de conductas que no se incluyan en el ámbito de aplicación del presente procedimiento o informaciones de conductas cuando se evidencie que no son veraces, salvo que la falta de veracidad dé lugar a un procedimiento judicial.

Todos los datos de aquellas informaciones sobre las que, transcurridos 3 meses desde su recepción, no se hayan iniciado actuaciones de investigación, deberán ser suprimidos del Sistema, salvo que sean necesarios para evidenciar el funcionamiento del Sistema Interno de Información.

4.5.2. Información de datos personales

En materia de protección de datos personales, serán de aplicación las siguientes normativas:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales
- Título VI 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.

El tratamiento de datos personales, en los supuestos de comunicación internos, se entiende lícito en virtud de lo que disponen los artículos 6.1.c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 8 de la Ley Orgánica 3/2018, de 5 de diciembre, y 11 de la Ley Orgánica 7/2021, de 26 de mayo, cuando, de acuerdo con lo establecido en los artículos 10 y 13 de la presente ley, sea obligatorio disponer de un sistema interno de información.

El tratamiento de datos personales derivado de una revelación pública se presumirá amparado en lo dispuesto en los artículos 6.1.e) del Reglamento (UE) 2016/679 del

Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 11 de la Ley Orgánica 7/2021, de 26 de mayo.

El tratamiento de las categorías especiales de datos personales por razones de un interés público esencial se podrá realizar conforme a lo previsto en el artículo 9.2.g) del Reglamento (UE) 2016/679.

Cuando los datos se obtengan directamente de la persona interesada, se le facilitará la siguiente información:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable 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 transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

Además de la información mencionada anteriormente, el responsable del tratamiento facilitará a la persona interesada, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo de conservación de los mismos o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos a la persona interesada, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos; en caso de que la persona investigada ejerza el derecho de

oposición al tratamiento de sus datos personales se entiende que existen motivos legítimos imperiosos que legitiman continuar con dicho tratamiento (art. 21.1. RGPD y art. 31.4 Ley 2/2023).

c) el derecho a presentar una reclamación ante una autoridad de control;

d) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si la persona interesada está obligada a facilitar los datos personales y está informada de las posibles consecuencias de que no facilitar tales datos;

f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4 (RGPD), y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

4.5.3. Tratamiento de datos personales en el Sistema Interno de Información

El acceso a datos personales contenido en el Sistema Interno de Información quedará limitado a:

- Persona Responsable del Sistema Interno de Información y, a quien lo gestione directamente.

- Persona Responsable de RRHH o el órgano competente, cuando pudiera proceder la adopción de medidas disciplinarias contra el trabajador/a.

- Persona Responsable de Servicios jurídicos de la Empresa, siempre que proceda la adopción de medidas legales en relación con los hechos comunicados.

- Los encargados de tratamiento que eventualmente se designen.

- El Delegado de Protección de Datos, en caso de que se disponga del mismo.

Será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceras partes, cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación procediéndose, en su caso, a su inmediata supresión.

Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la ley.

Los datos personales relativos a las comunicaciones recibidas y a las investigaciones internas sólo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con la legislación aplicable. En ningún caso podrán conservarse los datos por un período superior a 10 años.

4.6. MEDIDAS DE PROTECCIÓN

4.6.1. Condiciones de protección para personas informantes

Todas las personas que comuniquen o revelen infracciones objeto del presente procedimiento tendrán derecho a protección cuando haya motivos razonables para pensar que la información aportada es veraz en el momento de la comunicación o revelación, aun cuando no se aporten pruebas concluyentes, pero siempre que se haya realizado respetando lo previsto en el presente procedimiento y en la normativa vigente.

No dispondrán de derecho de protección todas aquellas personas que comuniquen o revelen:

- Informaciones contenidas en comunicaciones que hayan sido inadmitidas en canales internos o externos de información.

- Informaciones vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiere la comunicación.

- Informaciones que ya se encuentren disponibles para el público o que constituyan meros rumores.

- Informaciones sobre acciones u omisiones no contempladas en el presente procedimiento.

4.6.2. Prohibición de represalias

Quedan prohibidos los actos constitutivos de represalias, sean amenazas o tentativas, contra las personas informantes, entendiendo por represalias todas aquellas prohibidas por ley, así como cualquier trato desfavorable en el contexto laboral o profesional simplemente por su condición de informante o por haber realizado una revelación pública.

De manera general, se consideran represalias:

a. suspensión, despido, destitución o medidas equivalentes.

b. no renovación o terminación anticipada de un contrato de trabajo temporal.

c. terminación anticipada o anulación de contratos de bienes o servicios.

d. imposición de cualquier medida disciplinaria, amonestación u otra sanción, incluidas las sanciones pecuniarias.

e. degradación o denegación de ascensos; y cualquier otra modificación sustancial de las condiciones de trabajo.

f. no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que la persona trabajadora tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido.

g. daños, incluidos a su reputación, en especial en los medios sociales, o pérdidas económicas, incluidas la pérdida de negocio y de ingresos.

h. coacciones, intimidaciones, acoso u ostracismo.

i. evaluación o referencias negativas con respecto a sus resultados laborales.

j. inclusión en listas negras sobre la base de un acuerdo sectorial, informal o formal, que pueda implicar que en el futuro la persona no vaya a encontrar empleo en dicho sector.

k. anulación de una licencia o permiso.

l. denegación de formación.

m. discriminación, o trato desfavorable o injusto.

La persona que viera lesionados sus derechos por causa de su comunicación o revelación una vez transcurrido el plazo de dos años podrá solicitar la protección de la autoridad competente que, excepcionalmente y de forma justificada, podrá extender el período de protección, previa audiencia de las personas u órganos que pudieran verse afectados. La denegación de la extensión del período de protección deberá estar motivada.

Los actos administrativos que tengan por objeto impedir o dificultar la presentación de comunicaciones y revelaciones, así como los que constituyan represalia o causen

discriminación tras la presentación de aquellas al amparo de esta ley, serán nulos de pleno derecho y darán lugar, en su caso, a medidas correctoras disciplinarias o de responsabilidad, pudiendo incluir la correspondiente indemnización de daños y perjuicios a la persona perjudicada.

4.6.3. Medidas de apoyo

A las personas que comuniquen o revelen infracciones a través de los procedimientos previstos se les dará acceso a las medidas de apoyo siguientes:

a. Información y asesoramiento completos e independientes, que sean fácilmente accesibles para el público y gratuitos, sobre los procedimientos y recursos disponibles, protección frente a represalias y derechos de la persona afectada.

b. Asistencia efectiva por parte de las autoridades competentes ante cualquier autoridad pertinente implicada en su protección frente a represalias, incluida la certificación de que pueden acogerse a protección al amparo de la presente ley.

c. Asistencia jurídica en los procesos penales y en los procesos civiles transfronterizos de conformidad con la normativa comunitaria.

d. Apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la Autoridad Independiente de Protección de la persona informante, A.A.I., tras la valoración de las circunstancias derivadas de la presentación de la comunicación.

4.7. Régimen Disciplinario

En el caso de confirmarse la falsedad de la información, la persona infractora puede tener como consecuencia la exigencia de responsabilidades y/o sanciones derivadas de la legislación aplicable y/o del régimen disciplinario establecido en el Convenio colectivo correspondiente.

5. Canales Externos De Información

Además del presente canal interno, están disponibles los canales externos de información, para informar de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación de la Ley 2/2023, ante la Autoridad Independiente de Protección del Informante, A.A.I., ante las autoridades u órganos autonómicos correspondientes, y, cuando proceda, a instituciones, organismos o agencias de la UE a través de los siguientes links:

- Canal establecido por la Autoridad Independiente de Protección del Informante
- Servicio Nacional de Coordinación Antifraude (S.N.C.A.)

  https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/Paginas/ComunicacionSNCA.aspx
- Oficina Europea de Lucha contra el Fraude (OLAF)

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

  https://www.eppo.europa.eu/en/reporting-crime-eppo
- Dirección de Competencia de la Comisión Nacional de los Mercados y la Competencia

  https://edi.cnmc.es/buzones-anonimos/sica