CANAL INTERNO DE INFORMACIÓN

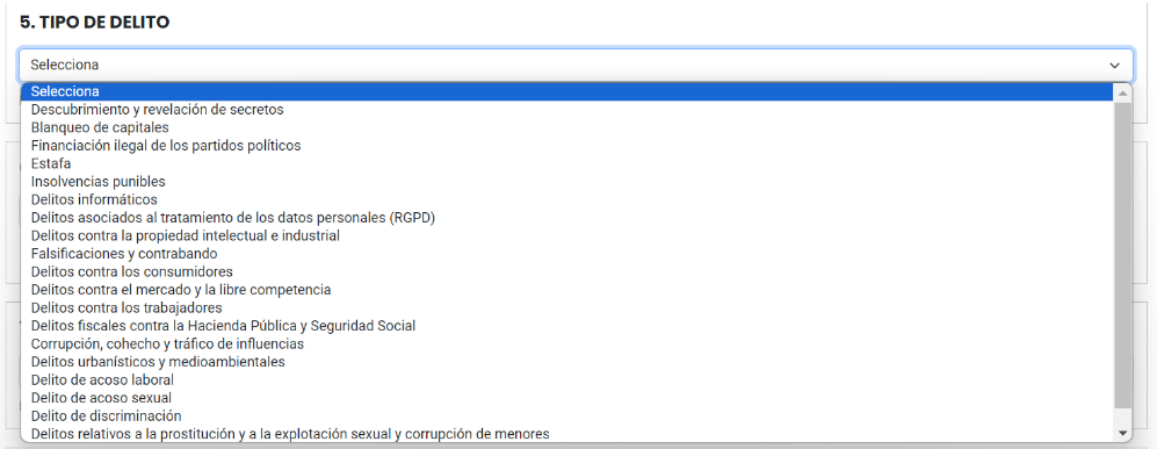
INDICE

1. Contenido de la Comunicación

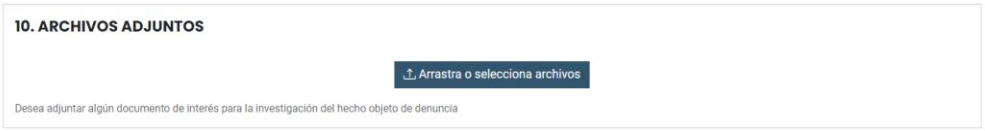
La comunicación o denuncia que se presente, a través del formulario dispuesto para tal efecto en el "canal interno de información", deberá contener la máxima información posible (indicios, pruebas, testigos, etc.), así como los datos identificativos, si se pueden aportarlos, asociados a las personas que han realizado conductas contrarias al ordenamiento jurídico, normas administrativas y código ético. Se deberán aportar los siguientes datos, en los campos establecidos para tal efecto, en dicho formulario:

- Nombre y apellidos, NIF (en caso de que lo conozca), centro de trabajo, área funcional, puesto de trabajo que desempeña y otros datos de los que se disponga que permita identificar a la persona o las personas que se relacionan con el hecho comunicado asociado a una infracción o delito, de acuerdo con el desplegable que se propone en el punto 5 "tipo de delito" [1].

[1] Captura de pantalla del punto 5 del formulario del "Canal de denuncias 360º", con su desplegable asociado a delitos referenciados con la finalidad de que el informante pueda encuadrar los hechos o actuaciones por él conocidas



- Descripción detallada de los hechos y conductas (comisión u omisión) realizadas por personal de **SPM SEGURIDAD**, que puedan constituir algún tipo de infracción o delito. Será relevante para la "evaluación de la comunicación o denuncia" y posterior investigación, si así se considera, aportar aquella documentación de que se disponga a través del punto 10 "archivos adjuntos" [2].



2. Tramitación de la comunicación

Con carácter general, alineado con lo establecido en la Ley 2/2023, en cuanto al procedimiento de gestión de una información o denuncia, una vez recibida la comunicación en cuestión, esta pasará por diferentes estados, en función del alcance de la misma:

- Recepción [3]
- Registro [3]
- Valoración, con objeto de realizar un análisis, que posteriormente determinará el "archivo" o "admisión a trámite" de la comunicación.
- En su caso, si es "admitida a trámite", se establecerá un proceso de investigación (instrucción), con los datos y hechos contenidos en la misma pudiéndose acordar el inicio de las actuaciones que procedan.

[2] Captura de pantalla del punto 10 del formulario (permite la subida de archivos/documentos).

- Una vez finalizado el proceso de investigación, se procederá a emitir una resolución que conllevará medidas o actuaciones necesarias, en el caso que se haya podido verificar una infracción o delito.

2.1 Externalización parcial de la gestión

SPM SEGURIDAD con la finalidad de reforzar la independencia, la objetividad y el respeto a las garantías asociadas al proceso de gestión de las comunicaciones, ha considerado parcialmente externar el proceso con un experto externo [3], de acuerdo con lo determinado en el art. 6 de la Ley 2/2023 de protección al informante, lo que refuerza la objetividad y el debido tratamiento de todas las informaciones.

Las comunicaciones se resuelven utilizando un procedimiento riguroso, transparente y objetivo, salvaguardando en todo caso la confidencialidad de los interesados e involucrados en la comunicación o denuncia.[3]

3. Responsable del Sistema Interno de Información

Se ha considerado establecer, en este momento, como "Responsable del Sistema Interno de Información" de SPM al Responsable del Departamento Administración, en los términos establecidos en la Ley 2/2023 de Protección al Informante en su artículo 8.

Es de interés establecer, en este punto, que el Sistema Interno de Información:

1. Estará integrado por:
   - Un canal interno de recepción de informaciones (formulario/aplicación)
   - Un procedimiento o manual determinando como se realizará la gestión dichas informaciones (que ha sido aprobado por el Órgano de Dirección)
   - Una persona responsable de la gestión y tramitación de la comunicaciones (Gestor)

2. El Sistema debe ofrecer plenas garantías de independencia, confidencialidad, seguridad y de que quienes acudan al canal interno no sufran represalias.

4. El Responsable del Sistema deberá desarrollar sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad u organismo, no podrá recibir instrucciones de ningún tipo en su ejercicio, y deberá

[3] El proceso de recepción y registro de una comunicación se encuentra externalizado a través de un tercero, Compliance Quality Legal Service S.L [www.qualitylegalservice.com], con el objeto de fundamentar los principios de confidencialidad y de protección al informante.

disponer de todos los medios personales y materiales necesarios para llevarlas a cabo.

5. En el caso del sector privado, el Responsable del Sistema persona física o la entidad en quien el órgano colegiado responsable haya delegado sus funciones, será un directivo de la entidad, que ejercerá su cargo con independencia del órgano de administración o de gobierno de la misma. Cuando la naturaleza o la dimensión de las actividades de la entidad no justifiquen o permitan la existencia de un directivo Responsable del Sistema, será posible el desempeño ordinario de las funciones del puesto o cargo con las de Responsable del Sistema, tratando en todo caso de evitar posibles situaciones de conflicto de interés.

6. En las entidades u organismos en que ya existiera una persona responsable de la función de cumplimiento normativo o de políticas de integridad, cualquiera que fuese su denominación, podrá ser esta la persona designada como Responsable del Sistema, siempre que cumpla los requisitos establecidos en esta Ley

4. Garantía de Confidencialidad: La identidad del Informante y de la persona Afectada

4.1 Confidencialidad de la identidad del informante

Este “canal interno” está diseñado, establecido y gestionado de forma segura de manera que se garantice la confidencialidad de la identidad del informante, así como la protección de los datos a los que se refiere la información, por lo que se impide el acceso a la misma por parte del personal no autorizado (los procesos de recepción y registro están externalizados). Esto se aplicará a cualquier dato del que se pueda deducir directa o indirectamente la identidad del informante.

La identidad del informante, siempre que el mismo no haya considerado su anonimización, sólo podrá ser comunicada, en el caso que resulte legalmente exigible, a la Autoridad Judicial Competente, a la Fiscalía correspondiente o a la Autoridad Administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora, lo que se trasladará al informante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial.

4.2 Confidencialidad de la Identidad de la persona a la que se refiera la información

A la persona a la que se refiere la información comunicada se le garantizará la confidencialidad de sus datos personales, con el objeto de evitar la posible difusión de los mismos. A estos efectos, el canal de información está diseñado, establecido y gestionado de forma segura de manera que garantice la confidencialidad de la identidad de la persona afectada por la información y la protección de los hechos y datos del procedimiento, por lo que se impide el acceso a la información por parte del personal no autorizado.

5. Protección del informante en al ámbito de la Ley 2/2023

Las personas que dentro del ámbito laboral o profesional se comuniquen con **SPM SEGURIDAD** a través de este canal interno (formulario), tendrán derecho a una serie de medidas de protección tal y como se recogen en la Ley 2/2023 de Protección al Informante (en adelante Ley).

De acuerdo con esta Ley, se prohíbe cualquier acto constitutivo de represalia, como pueden ser amenazas o tentativas de represalia al informante, extensiva a personas relacionadas con este.

De acuerdo con lo recogido en el artículo 36.3 de la Ley se entiende por represalia cualesquier acto u omisión que, de forma directa o indirecta, supongan un trato desfavorable al informante y que sitúe al mismo en desventaja ante la organización o terceros, sólo por su condición de informante.

Las medidas de protección serán extensibles a las personas que, en el marco de la representación legal de las personas trabajadoras, den soporte al informante en el proceso, así como las personas físicas relacionadas con el informante tales como compañeros de trabajo o familiares.

5.1 Derechos

Al informante se le garantizará el efectivo ejercicio de los siguientes derechos, sin perjuicio de cualesquiera otros que les reconozca la Constitución Española y el actual marco jurídico del Estado Español:

a) A presentar informaciones de modo anónimo y a que se mantenga el anonimato durante el procedimiento.

b) A indicar un domicilio, correo electrónico o lugar seguro donde recibir las comunicaciones que realice el Responsable del Sistema.

c) A comparecer ante el Responsable del Sistema o el gestor delegado por iniciativa propia.

d) A la renuncia de comunicarse con el Responsable del Sistema o el gestor delegado que instruya el procedimiento y, en su caso, a la revocación de dicha renuncia en cualquier momento.

e) A la preservación de su identidad.

f) A la protección de sus datos personales.

g) A conocer la identidad del gestor delegado que instruya el procedimiento.

h) A la confidencialidad de las comunicaciones.

i) A las medidas de protección y de apoyo en los términos previstos en la Ley 2/2023.

j) A presentar reclamación ante la Autoridad Independiente de Protección del Informante (AAI). En este momento no está creada dicha Autoridad (data 18/02/2024).

6. ¿Puede el informante acudir a otros canales alternativos?

Además de este “Canal interno”, circunscrito a la Ley 2/2023, que se propone por parte de SPM, existen otros canales internos a los que pueden acudir el personal o aquellos terceros que estén o hayan estado en contacto con SPM por motivo de su actividad laboral (con impacto en los derechos contemplado en el Estatuto de las personas trabajadoras) para comunicar cualquier información sobre posibles infracciones. Dicho canal en este momento es:

6.1 Ámbito Interno

El Departamento de RRHH (administracion@spmseguridad.com) está designado para atender asuntos asociados a acosos laboral, sexual, por razón de género o discriminación.

Establecer que la Responsable de Recursos Humanos cuenta con formación en materia de igualdad, y la misma persona se integra en la denominada Unidad de Atención al Acoso y Unidad de Instrucción del Acoso, por lo que cualquier comunicación

en este ámbito la podrá formular a esta persona, si así lo considera, de forma verbal o a través de su correo electrónico. Es de interés establecerle que está persona guardar confidencialidad y secreto en relación con la comunicación que usted haga.

7. Confidencialidad y protección de datos personales

7.1 Confidencialidad

De acuerdo con lo recogido 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, el canal de información garantiza la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la protección de datos, impidiendo el acceso de personal no autorizado y sin que su identidad pueda ser revelada a terceras personas. La persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante.

7.2 Cumplimiento del marco normativo en materia de tratamiento y protección de los datos personales

Los tratamientos de datos personales que se deriven de la tramitación del presente procedimiento de gestión de informaciones se realizarán de conformidad con lo dispuesto en el Titulo VI de la Ley 2/2023.

El “sistema interno de información” debe impedir el acceso no autorizado y preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado.

La identidad del informante solo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la Autoridad Administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora, y estos casos estarán sujetos a las salvaguardas establecidas en la normativa aplicable.

Si la información recibida contuviera categorías especiales de datos, se procederá a su inmediata supresión, salvo que el tratamiento sea necesario por razones de un interés público esencial conforme a lo previsto en el artículo 9.2.g) del Reglamento general de protección de datos, según dispone el artículo 30.5 de la Ley 2/ 2023.

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

En todo caso, transcurridos 3 meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema. 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 prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.