

Protocolo de Funcionamiento del Sistema Interno de Información

La Directiva 2019/1937/UE, de 23 de octubre, tiene por objetivo establecer unos parámetros comunes en la protección a las personas que informen sobre infracciones del Derecho de la Unión Europea, imponiendo la obligación de disponer de canales de denuncia como un medio para la consecución de un fin superior, vinculado a erradicar prácticas indeseadas en la gestión de organizaciones públicas y privadas, y reforzando una estrategia de integridad con las medidas que se adopten en esta materia.

La Directiva ha sido objeto de trasposición con 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 cual parte de la premisa de que la colaboración ciudadana resulta indispensable para la eficacia del Derecho, colaboración que se proyecta sobre el deber de los trabajadores, funcionarios y profesionales de informar de las irregularidades de que tengan conocimiento en el contexto de su relación laboral y profesional, con el objetivo de prevenir prácticas fraudulentas y corruptas.

La exigencia de la normativa respecto a los canales de denuncia interna es que se integren con procedimientos que permitan garantizar el seguimiento diligente de las denuncias, conformando así un conjunto integrado bajo la autoridad de un responsable del Sistema Interno de Información.

1. Irregularidades e infracciones susceptibles de ser informadas.

Con la aprobación del presente Protocolo se persigue una doble finalidad: por un lado, fomentar el ejercicio de actuaciones *ad intra* que favorezcan la posibilidad de informar de las categorías de irregularidades de las que el informante haya tenido conocimiento en el contexto de la relación laboral o profesional que mantiene o ha mantenido con Grupo Previsión Sanitaria Nacional (en adelante, Grupo PSN o Grupo) y, por otro, articular el procedimiento y requisitos para su utilización, con pleno respeto a los principios y directrices de la Ley de protección del informante.

Respecto a las diversas categorías de irregularidades e infracciones legalmente previstas, se extiende la protección a las personas que informen sobre infracciones del Derecho de la UE que afecten a los intereses financieros de la misma, a su mercado interior, o las que entren dentro del ámbito de aplicación de los actos de la UE en determinados sectores concretos como contratación pública, servicios financieros, prevención del blanqueo de capitales y de la financiación del terrorismo, seguridad de los productos comercializados, seguridad del transporte, protección del medio ambiente, protección frente a las radiaciones y seguridad nuclear, cadena alimentaria, sanidad animal y bienestar de los animales, salud pública y protección de los consumidores, protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información; así como a las acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave.

En lo que al Grupo se refiere y teniendo en cuenta sus particularidades, sin ánimo de exhaustividad, las informaciones que pueden canalizarse a través del Sistema de Información podrán versar sobre las materias a las que se refiere el apartado 2 de la Política del Sistema Interno de Información y Defensa del Informante de Grupo PSN (en adelante, la Política), a través del Sistema de Información relativo a la normativa sobre protección de las personas que informen sobre infracciones del Derecho de la UE, que el Grupo pone a disposición para comunicar cualquier vulneración de la citada normativa que no tenga un canal específico de comunicación.

La protección no sólo opera en los supuestos en que se informe de irregularidades que ya se han cometido, sino también de aquellas otras que todavía no se han materializado en todos sus extremos, o incluso si se informa de conductas encaminadas a ocultar esas irregularidades.

No estarían amparadas por esa protección, de acuerdo con el apartado 3 del presente Protocolo:

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

- Informaciones que se refieran a acciones u omisiones no comprendidas en el artículo 2 de la Ley 2/2023.
- Informaciones sobre irregularidades que ya estén completamente disponibles para el público, o que no contengan información nueva respecto de otras anteriores.
- Informaciones que no sean más que meros rumores o que carezcan de toda verosimilitud y las que se hayan obtenido mediante la comisión de un delito.

A través de este Sistema se presentarán comunicaciones o informaciones diferentes de las anteriormente previstas para las entidades en que resulte de aplicación; concretamente, las relativas a la prevención penal en relación con los posibles delitos contenidos en el “Anexo: Materias canal de denuncias en el ámbito penal”, incluido en el presente documento, siempre que no afecten a las materias anteriores.

Las comunicaciones relacionadas con la prevención del blanqueo de capitales y la financiación del terrorismo (PBCyFT), excluyendo la comunicación de operaciones sospechosas cuando exista indicio o certeza de que están relacionadas con el blanqueo de capitales y/o con la financiación del terrorismo, de acuerdo con el apartado 2 de la Política, las relativas a las posibles infracciones en materia de distribución de seguros, las relativas a la privacidad y la protección de datos y las relativas al acoso y discriminación en el empleo, se comunicarán a través de los canales pertinentes de acuerdo con la Política. No obstante, sus remitentes no serán beneficiarios de la protección dispensada por la Ley 2/2023.

2. Informantes susceptibles de ser protegidos.

Este protocolo protegerá a todas las personas que informen y pertenezcan a cualquiera de los colectivos indicados el apartado 2 de la Política.

3. Condiciones de protección de los informantes.

Los informantes tendrán derecho a protección en virtud del presente Protocolo siempre que:

1. Quien comunica la infracción tenga motivos razonables para pensar en ese momento que dicha información es veraz a la luz de las circunstancias y de la información de que disponga en el momento de presentarla. Aunque no se aporten pruebas concluyentes, es suficiente que se planteen dudas o sospechas razonables. No obstante, quedarán exentos de la protección quienes comuniquen información que ya esté completamente disponible para el público, o rumores y habladurías no confirmados.

Los motivos personales o profesionales de quienes denuncian las irregularidades deben ser irrelevantes para determinar si esas personas deben recibir la protección que otorga la regulación.

2. La comunicación de la infracción o irregularidad debe realizarse a través del Sistema Interno de Información establecido por Grupo PSN.

Se otorgará también protección a quien revele públicamente infracciones si, tras realizar la comunicación, primero por canales internos y externos, o directamente por canales externos, no se hayan tomado medidas apropiadas al respecto en el plazo establecido y se tengan motivos razonables para pensar que la infracción puede constituir un peligro inminente o manifiesto para el interés público (en particular cuando se da una situación de emergencia, o existe un riesgo de daños irreversibles, incluido un peligro para la integridad física de una persona); o también cuando, en caso de comunicación a través de un canal externo de información, exista riesgo de represalias o haya pocas probabilidades de que se dé un tratamiento efectivo a la información debido a las circunstancias particulares del caso, tales como ocultación o destrucción de pruebas o connivencia de una autoridad con el autor de la infracción.

4. Procedimiento de gestión del Canal de información sobre infracciones (Ley 2/2023).

Este procedimiento tiene por objeto profundizar en el conocimiento de los hechos comunicados por el informante para valorar de forma preliminar la exactitud y trascendencia de los mismos, por cuanto la investigación que se desarrolle en este ámbito debe restringirse, tanto en su contenido, como en su duración, a lo estrictamente necesario a tales fines.

4.1. Acceso y funcionamiento del Canal.

El Sistema Interno de Información será accesible a través de la página web del Grupo PSN. Dicho Sistema será único para todas las empresas del Grupo, si bien permitirá asignar cada comunicación a la Entidad a la que se refieren los hechos objeto de la misma. El informante que desee mantenerse en el anonimato podrá hacerlo con las garantías suficientes establecidas en la Política.

El conjunto de actividades de las distintas entidades para el registro, admisión a trámite, comprobación y resolución de las comunicaciones recibidas se desarrollará en el plazo más breve posible, atendiendo a las características de los hechos comunicados y las demás circunstancias concurrentes.

Las comunicaciones podrán realizarse:

- Por escrito: De acuerdo con el formulario habilitado al efecto para ello en el Sistema Interno de Información o, en su caso, por carta.
- Verbalmente: a través de los sistemas de mensajería de voz del Sistema de Información, o, previa solicitud del informante, por medio de reunión presencial, a celebrar en el plazo de 7 días naturales.
- De ambos modos, por escrito o verbalmente.

Se advertirá al informante de que la comunicación será grabada, en su caso, con arreglo a la legislación que resulte de aplicación, y de que sus datos personales serán tratados conforme a la normativa de protección de datos, y recibirá acuse de recibo de la comunicación o información realizada en el plazo de los siete días naturales siguientes a su recepción.

4.2. Registro y clasificación de las denuncias.

Todas las comunicaciones recibidas se analizarán de forma independiente y se garantizará la confidencialidad de la identidad de la persona que la plantea y del denunciado o denunciados.

Una vez recibida la comunicación, el Sistema le asignará un código de identificación, correlativo, y se incorporará a una base de datos, en la que se registrará la calificación dada a dicha comunicación y su estado de tramitación, que se actualizará a lo largo de las distintas fases del procedimiento.

Al informante se le facilitará un justificante de la presentación y registro de la comunicación realizada, a efectos de acreditar el cumplimiento del deber general de cooperación a que se refiere el apartado 7 de la Política.

Las denuncias se deberán clasificar por orden de importancia del 1 al 5, siendo 1 aquellas consideradas más relevantes y 5 las menos relevantes. Como aspectos considerados de mayor relevancia se considerarán las situaciones siguientes: las que puedan dar lugar a eventuales responsabilidades penales de la entidad o sus directivos, incluyendo (pero sin limitarse) aquellas que puedan involucrar actos que, de confirmarse, pudieran llegar a ser clasificadas como corrupción en el ámbito público en alguna de sus formas; en las cuales exista el riesgo de vulnerar alguna legislación vigente; situaciones que, de conocerse fuera de la entidad, pudieran causar un daño a la imagen del Grupo; que supongan un riesgo en la continuidad del negocio, un importe elevado asociado a la denuncia fundada o un número de personas o áreas afectadas por los hechos denunciados.

La valoración indicada en este apartado determinará la prioridad a la hora de comenzar la revisión de la misma y la asignación de los recursos. Una vez realizado el análisis preliminar de la comunicación, se indicará su nivel con carácter provisional, pudiendo variar en función de la obtención de nuevos datos o indicios, documentándose debidamente.

Las comunicaciones recibidas en el canal se clasificarán conforme a su naturaleza y de acuerdo con las categorías indicadas. Dicha clasificación podrá ser objeto de actualización conforme evolucionen las necesidades de información al respecto.

Las denuncias que se reciban a través del Sistema Interno de Información y que guarden relación con situaciones de discriminación, acoso moral (mobbing) y acoso sexual o por razón de género, se tramitarán, en su caso, de

conformidad con los procedimientos específicos que puedan existir para estas materias concretas en la sociedad empleadora del informante.

4.3. Análisis preliminar de los hechos.

Recibida una comunicación, el responsable del Sistema determinará si procede o no darle trámite, considerando si reúne los requisitos mínimos para ello. En el supuesto de que la comunicación sea manifiestamente infundada o que, siendo anónima, no aporte información suficiente para la comprobación de los hechos denunciados, no será admitida a trámite, documentándose tal decisión.

En caso de que los hechos pudiesen afectar a más de una sociedad del Grupo o a profesionales adscritos a varias de ellas, la comunicación se remitirá por cualquiera de las sociedades afectadas al responsable para que adopte las medidas de coordinación oportunas, incluyendo la avocación de la decisión sobre su admisión a trámite.

4.4. Comprobación de los hechos.

De acuerdo con el análisis preliminar, el responsable procederá a la comprobación y análisis de los hechos para lo que se podrá requerir, en su caso, la colaboración de otras áreas o de terceros si fuera necesario.

En toda actuación regirá el principio de presunción de inocencia y la protección del honor de las personas afectadas.

Dada la alarma social que puede producir este tipo de situaciones y los perjuicios que pueden ocasionar al trabajador/es afectados y al objeto de tomar las acciones oportunas, en su caso, esta fase deberá durar el tiempo estrictamente necesario para el esclarecimiento de los hechos, siendo recomendable que sea sumaria, sin perjuicio de todas las garantías que se puedan requerir en tal fase, que se iniciará con el trámite de audiencia a todos los intervinientes, practicándose cuantas diligencias puedan considerarse oportunas, conducentes al esclarecimiento de los hechos acaecidos, otorgando a la persona/s afectadas por la información el derecho ser informada de las acciones u omisiones que se le atribuyen, y a ser oída en cualquier momento, formulando cuantas alegaciones consideren convenientes, en un plazo máximo de 15 días naturales, desde la recepción del escrito de denuncia. Cuando proceda se tomará declaración inmediata, verbal o por escrito, a compañeros o posibles testigos que se considere puedan aportar alguna información sobre los hechos, sin que se facilite información a partes no implicadas en el caso, procediendo en todo momento con la discreción necesaria con el fin de proteger la dignidad y confidencialidad de todos los implicados.

El Sistema permitirá mantener la comunicación con el informante y, si se considera necesario, se le solicitará información adicional, debiendo asegurar un adecuado cumplimiento de la legislación de protección de datos aplicable y en particular, respecto a los derechos de los titulares de dichos datos.

Se recabará cuanta información se considere sea útil para el esclarecimiento de los hechos, proceso que se sustanciará en un plazo máximo de 15 días naturales, guardando una absoluta confidencialidad y reserva, por afectar directamente a la intimidad y honorabilidad de las personas.

El responsable del Sistema será el encargado de recibir, registrar, tramitar, investigar, gestionar y dar respuesta sobre las informaciones recibidas. La investigación que se desarrolle a los efectos de esclarecer los hechos debe restringirse, tanto en su contenido como en su duración, a lo estrictamente necesario.

El plazo máximo para dar respuesta al informante no podrá ser superior a tres meses a contar desde la recepción de la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, este podrá extenderse hasta un máximo de otros tres meses adicionales.

4.5. Resolución.

Concluida la fase de investigación sobre los hechos denunciados, se alcanzarán unas conclusiones que se podrán formalizar en un informe. A la vista de toda la información obtenida durante el proceso de investigación, pueden darse las siguientes situaciones:

- Que se considere no acreditada la existencia de infracción o comisión de irregularidad alguna, acto contrario a la legalidad o a las normas internas, en cuyo caso se acordará dar por concluido el expediente sin necesidad de adoptar ninguna medida, procediéndose a su archivo, documentando tal decisión.
- Que no haya indicios racionales de encontrarse ante una presunta situación denunciada, pero sí haya indicios de encontrarse ante una presunta falta laboral de otra índole, en cuyo caso se pondrá en conocimiento de la Dirección de Recursos Humanos, al objeto de que se incoe el preceptivo expediente disciplinario, y, una vez finalizado el mismo, proceda a la sanción correspondiente, en su caso, de igual forma que si se hallasen indicios racionales de encontrarse ante una presunta situación ilícita, en su caso.

Del resultado de todas las actuaciones se deberá informar por escrito tanto al informante como al/los denunciados.

Con independencia del resultado obtenido en el procedimiento, se procurará que en las resoluciones del mismo se contemplen medidas tendentes a la mejora, prevención y supresión de las situaciones que se hayan podido producir y que sean objeto del presente Protocolo.

Cuando indiciariamente los hechos pudieran ser constitutivos de delito, el responsable del Sistema remitirá la información al Ministerio Fiscal con carácter inmediato y a la Fiscalía Europea si afectasen a los intereses financieros de la UE. En caso de tratarse de una infracción administrativa grave o muy grave, se remitirá a la autoridad administrativa competente para profundizar en los hechos y resolver como proceda, siempre con las debidas garantías de defensa para el presunto responsable.

5. Protección de datos y conservación de la información.

Los tratamientos de datos personales derivados de esta Ley se regirán por el Reglamento 2016/679 y La Ley Orgánica 7/2021, sin que, de acuerdo con el apartado 6 de la Política, en ningún caso se recopilen datos personales cuya pertinencia no resulte manifiesta para tratar una información específica. En caso de accidente se eliminarán sin dilación indebida.

La licitud del tratamiento de los datos personales en los supuestos de comunicación internos se basará:

- En el cumplimiento de una obligación legal cuando sea obligatorio contar con un sistema de información legal aplicable al responsable del tratamiento.
- En los casos en que no sea obligatorio, en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

La información a facilitar a los interesados sobre datos obtenidos directamente de ellos será la siguiente: identidad y datos de contacto del responsable y del delegado de protección de datos; fines del tratamiento y base jurídica; destinatarios o categorías de destinatarios de los datos personales, en su caso; intención del responsable de transferir datos personales a un tercer país u organización internacional y existencia o ausencia de una decisión de adecuación, o, en el caso de las transferencias internacionales de datos, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición; plazo durante el cual se conservarán los datos personales o criterios utilizados para su determinación; existencia de decisiones automatizadas, incluida la elaboración de perfiles; si la comunicación de datos personales es un requisito legal, que está informado de las posibles consecuencias de no facilitar tales datos, y derecho a presentar una reclamación ante una autoridad de control.

Los interesados podrán ejercer los derechos de acceso, rectificación, supresión, limitación, notificación de la rectificación, supresión o limitación y la portabilidad.

En caso de ejercitarse el derecho de oposición, se presume la existencia de motivos legítimos para el tratamiento de los datos.

El acceso a los datos contenidos en el Sistema Interno de Información está limitado, dentro de sus competencias y funciones, exclusivamente, al Órgano de Gobierno y al responsable del Sistema Interno de Información, al

responsable de Recursos Humanos, cuando deba adoptar sanciones, al responsable de los Servicios Jurídicos, si proceden medidas legales, y al delegado de Protección de Datos, en lo relativo a esta materia

Será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la tramitación de los procedimientos sancionadores o penales.

En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios. Los datos que sean objeto de tratamiento podrán conservarse únicamente durante el tiempo imprescindible para decidir si iniciar o no la investigación. Transcurridos 3 meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su eliminación.

La información se alojará y conservará de acuerdo con los requerimientos legales que resulten de aplicación en cada caso.

6. Seguimiento del Protocolo.

Con el objeto de asegurar el cumplimiento del presente Protocolo se creará un órgano de seguimiento y gestión, formado por las personas que tienen acceso al mismo quienes, en su caso, emitirán un informe de conclusiones y propuestas de mejora.

ANEXO: MATERIAS CANAL DE DENUNCIAS EN EL ÁMBITO PENAL

CONDUCTA SUSCEPTIBLE DE SER COMETIDA POR LA ENTIDAD (PERSONA JURÍDICA)	REGULACIÓN CÓDIGO PENAL
Privacidad/seguridad de la información: Descubrimiento y revelación de secretos (acceso ilícito a datos y a procesos informáticos) y Daños informáticos	197 y 264
Empresa emisora de valores negociados: Falsar información económico-financiera Alteración de precios / Difusión de noticias o rumores / Utilización de información privilegiada. Abuso de información relevante sobre valores o instrumentos cotizados	282 bis, 284 y 285
Apoderamiento, difusión o divulgación de secretos de empresa	278 y ss.
Estafa y uso de bienes embargados sin autorización o su alzamiento para eludir responsabilidades civiles, Disposición de bienes en situación de insolvencia, alzamiento para favorecer a acreedores o presentación de datos contables falsos en proceso concursal	248 y ss. y 257 y ss.
Delitos relativos a Propiedad Intelectual Industrial	270 y ss.
Publicidad engañosa	282
Actos contrarios a la integridad de la Entidad: Corrupción entre particulares y a funcionario público y cohechos pasivo y activo, cometido por autoridad o funcionario público o frente a éste por particular, y tráfico de Influencias, por autoridad o funcionario público	286 ter y 419 y ss. 424 y ss. y 428
Blanqueo de capitales y Financiación del terrorismo y a partidos políticos	301 y 576 bis y 304 bis
Delitos contra la Hacienda Pública y la Seguridad Social, incluyendo incumplimiento de obligaciones contables establecidas por ley tributaria y fraude en subvenciones	305 y ss
Delitos sobre ordenación del territorio y urbanismo y contra los recursos naturales y el medio ambiente	319 y 325 y ss.
Delitos contra los trabajadores	173.1, 184.5 y 311 y ss.