

 **Open the whistle**



GUÍA DE INTEGRIDAD PARA INFORMANTES



Cofinanciado por
la Unión Europea

El proyecto «Open the Whistle: Proteger a los denunciantes de irregularidades a través de la transparencia, la cooperación y las estrategias de Gobierno Abierto» (OPWHI) es un proyecto cofinanciado por la Unión Europea (Proyecto: 101140801 - Convocatoria: CERV-2023-CHAR-LITI-WHISTLE) que pretende crear un entorno que apoye la denuncia protegida de infracciones del Derecho de la Unión y otras infracciones, promoviendo una cultura en la que los denunciantes puedan hablar con seguridad.

2025 Transparency International España

ISBN: 978-84-09-73335-4



Esta obra está bajo la licencia [Creative Commons Atribución-NoComercialSinObraDerivada 4.0 Internacional](https://creativecommons.org/licenses/by-nc-nd/4.0/).

Concepto gráfico y portada: Alessia Riolo

Diseño y maquetación: Álvaro Arribas Jiménez



**Cofinanciado por
la Unión Europea**

Cofinanciado por la Unión Europea. No obstante, los puntos de vista y opiniones expresados son exclusivamente los de los autores y no reflejan necesariamente los de la Unión Europea ni los de la Agencia Ejecutiva en el Ámbito Educativo y Cultural Europeo (EACEA). Ni la Unión Europea ni la EACEA pueden ser consideradas responsables de las mismas.

ENTIDADES PARTE DEL PROYECTO

Libera – Asociaciones y cifras contra las mafias (Libera - Associazioni e numeri contro le mafie) - Libera es una red de organizaciones de la sociedad civil comprometidas con la lucha contra la corrupción, el crimen organizado y sus facilitadores en Italia, y con el objetivo de promover la justicia social y la democracia. Fundada en Italia en 1995, la red incluye actualmente 278 grupos locales y 80 organizaciones internacionales en 35 países de Europa, los Balcanes Occidentales, África y América Latina. Desde 2016, participa activamente en la protección de los denunciantes, en particular a través de Línea Libera, un servicio de escucha y apoyo a potenciales informantes tanto del sector público como del privado. Libera colabora estrechamente con la Autoridad Nacional Anticorrupción italiana (ANAC), administraciones públicas, otras OSC y las comunidades locales para apoyar mejor a potenciales informantes y promover iniciativas compartidas contra la corrupción.

Universidad de Pisa (Università di Pisa - UNIPI) – Fundada a mediados del siglo XIV, la Universidad de Pisa es una de las universidades de mayor renombre en Europa. Desde 2010, el Departamento de Ciencias Políticas de la Universidad de Pisa organiza el Programa de Maestría en "Análisis, Prevención y Lucha contra el Crimen Organizado y la Corrupción", que ha formado a más de doscientos estudiantes de toda Italia y del extranjero en materia de lucha contra la corrupción y la mafia. Además, la UNIPI ha creado el Observatorio sobre la Corrupción Política.

Transparencia Internacional España (Transparency International España - TI-E) - TI-E nace en 2006 como respuesta de la sociedad civil a un escenario complejo en España, marcado por la falta de un marco regulatorio adecuado en materia de transparencia, integridad y buena gobernanza y de una cultura de la ética y la integridad. Desde entonces, TI-E ha liderado desde la sociedad civil la lucha contra la corrupción y por la transparencia, en lo público y en lo privado, para promover una ciudadanía informada y activa y fortalecer las instituciones y consolidar nuestra democracia, colaborando con todos los sectores de la sociedad para construir un entorno más justo y transparente. A través del seguimiento de las políticas públicas, la promoción y la investigación, TI-E aboga por una mayor transparencia e integridad en todos los ámbitos de la vida pública y participa activamente en el diseño, desarrollo, seguimiento y evaluación de políticas públicas en materia de prevención de la corrupción, transparencia, integridad y gobierno abierto, proporcionando una perspectiva transversal de género en todas sus acciones, identificando las desigualdades interseccionales y reconociendo los impactos diferenciados de la corrupción y la falta de transparencia.

Centro para el Estudio de la Democracia (Center for the Study of Democracy - CSD) - Fundado a finales de 1989, es un grupo de reflexión interdisciplinario orientado a la investigación con enfoque regional en Europa y los países de los Balcanes Occidentales. El CDS ha publicado una serie de informes, manuales y guías sobre la protección de los derechos humanos, el Estado de derecho y la lucha contra la corrupción. La organización participa activamente en la mejora de las políticas y la cultura

de denuncia de irregularidades como actor regional anticorrupción y miembro de la Coalición de Europa Sudoriental para la Protección de los Denunciantes (SECWP). El CDS aboga activamente por la transposición de la Directiva 2019/1937/UE sobre denuncia de irregularidades de la UE en Bulgaria. Sus expertos participaron en el grupo de trabajo del Ministerio de Justicia, que redactó la ley de transposición de la Directiva 2019/1937/UE, y formularon observaciones sobre todos los proyectos de ley presentados al Parlamento.

Autoridad Nacional Anticorrupción de Italia (Autorità Nazionale Anticorruzione - ANAC) – Creada en 2012, ANAC es la autoridad nacional italiana encargada de recibir denuncias e investigarlas, entre las cuales se encuentran aquellas que involucran represalias adoptadas contra informantes. ANAC protege la confidencialidad de los y las informantes y del contenido de las denuncias y garantiza el anonimato, mediante el uso del sistema de encriptación de una plataforma informática, puede comunicarse de forma anónima con el denunciante. La potestad sancionadora de ANAC incluye los casos de represalias, los casos de inacción de los funcionarios responsables que no han realizado ninguna verificación y análisis de las denuncias recibidas, y los casos de ausencia de un sistema de gestión de las denuncias.

Oficina Antifraude de Cataluña (Oficina Antifrau de Catalunya - OAC) - Es una institución de derecho público creada por la Ley 14/2008, de 5 de noviembre. Su finalidad es prevenir e investigar los casos de uso o asignación ilegal de fondos públicos o cualquier otra apropiación irregular derivada de actos que impliquen conflictos de interés o de utilización en beneficio privado de información derivada de las funciones inherentes a los servidores públicos. También brinda asesoramiento y formula recomendaciones para la adopción de medidas contra la corrupción, las prácticas fraudulentas y los comportamientos que atentan contra la integridad y la transparencia. También se han encomendado a la Oficina las funciones que la Ley Estatal 2/2023, de transposición de la Directiva 1937/2019/UE atribuye a la Autoridad Independiente de Protección de los informantes ante la OAC y la Oficina también puede ejercer sus competencias sancionadoras respecto a las infracciones de la Ley 2/2023, que regulaba la protección de las personas que informan sobre incumplimientos normativos y la lucha contra la corrupción.

Comisión de Protección de Datos Personales de Bulgaria (Komisiya za zashtita na lichnite danni Commission for Personal Data Protection - CPDP) – Creada en 2002, la Comisión Búlgara de Protección de Datos Personales es la autoridad nacional encargada de recibir las denuncias de irregularidades. El CPDP aplica la protección a las personas informantes teniendo en cuenta las condiciones, el procedimiento y las medidas de protección de informantes en los sectores público y privado que comunican información, o divulgan públicamente información sobre la legislación búlgara, o actos de la Unión Europea, que ponen en peligro o dañan el interés público y la legislación de la Unión Europea, así como los términos y condiciones para presentar y considerar dicha información o información divulgada públicamente.

AGRADECIMIENTOS

Los socios del proyecto desean agradecer las valiosas aportaciones de todas las personas que participaron en la elaboración de esta guía.

GRUPO DE TRABAJO

ANAC	Giulia Cossu Giovanni Paolo Sellitto Valentina Tomassi
CSD	Maria Yordanova Dimitar Markov
CPDP	Hristo Alaminov Yoan Angelov Atanaska Georgieva Kristina Radkova-Staneva Katya Stanimirova Radostina Takova Desislava Toshkova-Nikolova
Libera	Leonardo Ferrante Elisa Orlando Carlotta Bartolucci
OAC	Elisenda Escoda Marisa Miralles Òscar Roca Jordi Tres
TI-E	David Martínez García Ailén Rubio Arrieta Camila Cella Andrea Rivera
UNIPi	Alberto Vannucci Francesca Rispoli Martina Cataldo Eugenio Pizzimenti

COMITÉ CIENTÍFICO DEL PROYECTO

Laura Valli, ANAC
Massimiliano Andretta, UNIPi
Roberta Bracciale, UNIPi
Valentina Maria Donini, Scuola Nazionale dell'Amministrazione (SNA)
Ventsislav Karadjov, CPDP
Delyana Doseva, CSD
Elisabet Martínez, OAC
Silvina Bacigalupo Saggese, TI-E
Ramón Ragués i Vallès, UPF

ÍNDICE

INTRODUCCIÓN Y ESTRUCTURA DE LA GUÍA	PG. 7
CAPÍTULO 1: TRANSPARENCIA Y COMUNICACIÓN DE LOS SISTEMAS DE INFORMACIÓN	PG. 13
CAPÍTULO 2: INVESTIGACIÓN Y GESTIÓN ADECUADA EN LOS SISTEMAS INTERNOS DE DENUNCIA	PG. 34
CAPÍTULO 3: PROTECCIÓN DE DATOS PERSONALES	PG. 57
CAPÍTULO 4: PROTECCIÓN Y APOYO A LAS PERSONAS INFORMANTES	PG. 78
CAPÍTULO 5: MEDICIÓN Y EVALUACIÓN DE LA EFICACIA DEL SISTEMA Y EVALUACIÓN DE LA CULTURA DE DENUNCIA DE IRREGULARIDADES	PG. 93
CAPÍTULO 6: RECOMENDACIONES SOBRE GÉNERO Y GOBIERNO ABIERTO	PG. 109
MÁS ALLÁ DE LA GUÍA	PG. 112

INTRODUCCIÓN Y ESTRUCTURA DE LA GUÍA

CUÁL ES EL PROPÓSITO DE ESTA GUÍA

La presente Guía surge del conocimiento, la investigación y el trabajo de un grupo de autoridades, sector académico y organizaciones de la sociedad civil de **Italia**, **Bulgaria** y **España**. Su objetivo es proporcionar conocimientos teóricos y orientación práctica para establecer una nueva narrativa y un modelo de protección sólido para informantes, impulsando **un entorno seguro y de apoyo** para las personas informantes y facilitando la **denuncia efectiva de irregularidades**.

La Guía explora **cinco aspectos esenciales de la denuncia de irregularidades**, estructurada en cinco capítulos, que ofrecen nuevas perspectivas y recomendaciones para implementar **las mejores prácticas y fomentar una nueva narrativa** en torno a la denuncia de irregularidades y la protección de informantes:

- A. Capítulo 1 → Transparencia y comunicación de los sistemas de información
- B. Capítulo 2 → Investigación y gestión adecuadas dentro de los sistemas internos de denuncia de irregularidades
- C. Capítulo 3 → Protección de datos
- D. Capítulo 4 → Protección y apoyo a informantes
- E. Capítulo 5 → Medición y evaluación de la eficacia del sistema y evaluación del establecimiento de una cultura de denuncia de irregularidades

Además, esta Guía busca:

- A. Proporcionar información sobre **los mecanismos de denuncia estandarizados, las políticas y protocolos de los canales de información y las medidas de protección contra represalias y la confidencialidad**.
- B. Identificar retos en el marco de las leyes nacionales que transponen la **Directiva Europea 2019/1937/UE** 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 (**en adelante, "la Directiva"**) esforzándose por proporcionar respuestas para colmar algunas de lagunas existentes e impulsando la reflexión para aquellas cuestiones aún abiertas.
- C. Ofrecer un **análisis dinámico**, examinando la evolución de las respuestas a la Directiva e identificando **los retos actuales seis años después de su implementación**.
- D. Brindar **recomendaciones concretas basadas en las lecciones aprendidas durante estos años**, con el objetivo de identificar futuras mejoras.

Además, la guía identifica **mejores prácticas para promover una cultura de la transparencia, rendición de cuentas y responsabilidad ética**, fortaleciendo en última instancia las instituciones y aumentando la confianza pública.

LO QUE ESTA GUÍA NO ES

Conviene asimismo señalar que esta Guía no es:

- A. Un manual que proporciona un **análisis teórico en profundidad de la Directiva** ni **evaluaciones exhaustivas específicas de cada país**. Tampoco sirve como referencia definitiva para evaluar el cumplimiento efectivo de la ley por parte de los países analizados.
- B. Un documento de perspectiva única: no examina la denuncia de irregularidades únicamente desde un punto de vista legal, político o económico. En su lugar, **integra múltiples disciplinas y enfoques** para proporcionar una comprensión global, reconociendo la naturaleza multifacética de la **alerta de irregularidades y la protección de informantes**.
- C. Un análisis histórico o teórico: evita profundizar en la **historia o los fundamentos teóricos de la denuncia de irregularidades**, centrándose en cambio en **ideas y recomendaciones prácticas**.
- D. Una visión unilateral: sino que adopta una vocación práctica que no se centra únicamente en la funcionalidad del sistema de información ni exclusivamente en la protección de los denunciantes, sino que reconoce **la importancia de ambas perspectivas** y busca armonizarlas.

GOBIERNO ABIERTO Y GÉNERO: DOS ENFOQUES TRANSVERSALES NECESARIOS

A lo largo de los capítulos, la guía incorpora dos pilares transversales fundamentales: **enfoque de género y de gobierno abierto**.

- A. El **enfoque basado en el género** tiene como objetivo **generar conciencia** sobre la importancia de desarrollar sistemas de denuncia de irregularidades accesibles, inclusivos y **sensibles al género** para una denuncia y protección efectivas y completas. En los últimos años, ha habido un creciente reconocimiento de cómo las diferencias de género pueden afectar de manera desproporcionada a las mujeres, los hombres y otras identidades de género, lo que pone de relieve la necesidad de contar con mecanismos de denuncia de irregularidades sensibles al género. Ayuda a **abordar las brechas en la protección legal y las políticas** que tienden a no ser sensibles a la perspectiva de género y a menudo pasan por alto las consideraciones de diversidad, igualdad y no discriminación. En este contexto, la idea es **proporcionar herramientas tanto teóricas como prácticas** a todos los actores involucrados en la denuncia de irregularidades, facilitando la integración efectiva de un enfoque de género".

El enfoque de gobierno abierto tiene como objetivo formular recomendaciones para abordar los retos de la denuncia de irregularidades con base en los principios básicos del gobierno abierto, como la transparencia, la rendición de cuentas, la participación y la inclusión. Es decir, todas las acciones que la sociedad civil y las instituciones pueden emprender de manera colectiva y colaborativa para fomentar la denuncia de irregularidades y proteger a los denunciantes. Si su país es miembro de la Alianza para el gobierno abierto (OGP, por sus siglas en inglés), los autores sugieren que cualquier compromiso de este tipo forme parte de los ciclos del Plan de Acción Nacional¹, o del Desafío de gobierno abierto², que permite que se asuman y reconozcan compromisos de reforma ambiciosos fuera del ciclo regular del Plan de Acción. De esta manera, será más fácil establecer una relación transparente con todas las partes interesadas relevantes, co-crear soluciones y realizar un mejor seguimiento sobre su impacto.

POR QUÉ ES IMPORTANTE LA DENUNCIA DE IRREGULARIDADES Y LA PROTECCIÓN DE INFORMANTES.

"Whistleblowing" es un término anglosajón que entraña múltiples significados y matices. En términos generales, es una **"forma de denuncia"** que desempeña un papel crucial para garantizar la rendición de cuentas, exponer las malas prácticas y la corrupción, sacar a la luz las irregularidades ocultas y prevenir daños. Las personas informantes a menudo son testigos de irregularidades y actúan en el interés público para evitar daños, además, tienen derecho a un trato justo, respeto y **protección** contra represalias. Sin embargo, para que la denuncia de irregularidades sea realmente eficaz, **debe integrarse** como un **componente esencial y cultural** en los lugares de trabajo y en la sociedad.

Las protecciones legales sólidas, los mecanismos claros de denuncia y una cultura que fomente la **responsabilidad ética** son cruciales para empoderar a las personas para que hablen sin temor a represalias. En la actualidad, ciertas normas de comportamiento en las organizaciones y en la sociedad pueden desalentar a las personas de denunciar delitos o violaciones éticas: la necesidad de adaptarse, el concepto del denunciante **como espía o traidor**, o la idea de que la denuncia de irregularidades es una **"extrema ratio"** que requiere enormes esfuerzos legales pueden ser razones que disuadan a potenciales informantes. Esto es grave ya que, en lugar de ser visto como un elemento estructural de cualquier organización, todavía se ve como una **medida extraordinaria que requiere intervenciones excepcionales**. Al incorporar la denuncia de irregularidades como una práctica fundamental, creamos un entorno más seguro, transparente y responsable para todos.

¹ Ver: <https://www.opengovpartnership.org/process/action-plan-cycle/>

² Ver: <https://www.opengovpartnership.org/the-open-gov-challenge/open-government-challenge-areas/>

DOS PERSPECTIVAS DIFERENTES PERO COMPLEMENTARIAS

Este documento se esfuerza por equilibrar **dos perspectivas**:

- A Un enfoque "**centrado en la denuncia de irregularidades y los sistemas de información**".
- B Un enfoque "**orientado a la protección de las personas informantes**".

LA DIRECTIVA EUROPEA 2019/1937/UE Y SU TRANSPOSICIÓN

En 2016, la Comisión Europea declaró que **no existía base legal** alguna para adoptar una Directiva sobre denuncia de irregularidades, sin embargo, era más que patente la necesidad que había en toda Europa de una legislación armonizada de la UE sobre la protección de las personas informantes. Solo en 2019, en respuesta a una serie de **escándalos de alto perfil** (por ejemplo, LuxLeaks, Papeles de Panamá, etc.), el Parlamento Europeo y el Consejo adoptaron la Directiva de la UE 2019/1937 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. Su objetivo era claro: establecer un **estándar mínimo para la protección de los y las informantes en todos** los Estados miembros de la UE, garantizando que las personas que denunciaran infracciones del Derecho de la UE estuvieran protegidas **contra represalias**. Los Estados miembros de la UE tenían hasta **el 17 de diciembre de 2021** para transponer la Directiva a su legislación nacional. A partir de 2024, la mayoría de los Estados miembros han **ya transpuesto la Directiva a sus ordenamientos jurídicos**, aunque muchos de ellos se han enfrentado **a no pocas dificultades y retos** para garantizar el cumplimiento del espíritu de la misma. Así, la legislación nacional difiere ampliamente en cuanto a las condiciones en las que se protege a las personas informantes, así como su base jurídica en los distintos países.

DENUNCIA DE IRREGULARIDADES EN ITALIA

En **Italia**, el marco normativo de denuncia de irregularidades existía antes de la Directiva, con medidas iniciales introducidas en 2012 y luego ampliadas en 2017. La Ley 190/2012 fue la primera ley en **Italia** en introducir protecciones específicas para los denunciantes, aunque se limitó al sector público. Esta ley permitía a los empleados públicos denunciar conductas indebidas de las que tuvieran conocimiento en su lugar de trabajo sin sufrir represalias. Sin embargo, las protecciones eran débiles: el reglamento se limitaba a prohibir las sanciones disciplinarias contra informantes, pero no proporcionaba un sistema de protección cabal ni mecanismos claros para garantizar la confidencialidad. Además, no había salvaguardas para los empleados del sector privado. En 2017, la Ley 179 vino a fortalecer el marco al introducir protecciones más amplias tanto en el sector público como en el privado. Estableció medidas para garantizar la confidencialidad de los denunciantes e impuso sanciones a quienes intentaran tomar represalias contra ellos. Además, exigía a las empresas privadas que cumplieran determinados criterios que implementaran canales internos de denuncia.

Por último, en coherencia con la Directiva, la nueva ley de denuncia de irregularidades (Decreto Legislativo n.º 24/2023) obliga a las entidades públicas y privadas con más de 50 empleados a establecer canales internos de denuncia que garanticen la confidencialidad. De este modo, se pueden realizar denuncias a ANAC (el canal externo) si los canales internos son poco confiables, ineficaces o si la violación representa un riesgo público inminente. La ley ha introducido un reconocimiento a las organizaciones del tercer sector que apoyan a las personas informantes antes y después de la denuncia. La ley tiene como objetivo mejorar las salvaguardias contra las represalias y fortalecer los mecanismos de presentación de denuncias, extendiendo esta protección más allá de los empleados a los trabajadores independientes, voluntarios, pasantes, accionistas y facilitadores.

DENUNCIA DE IRREGULARIDADES EN BULGARIA

Antes de la adopción de la Directiva, **Bulgaria** contaba con disposiciones dispersas relacionadas con la protección de las personas denunciantes de irregularidades en diversas leyes. La Ley de Protección contra la Discriminación prohíbe las represalias contra las personas que presenten denuncias por discriminación, mientras que el Código de Procedimiento Administrativo ofrece salvaguardias generales para quienes denuncien abusos de poder o corrupción. Varios organismos participaron en la tramitación de esas denuncias, entre ellos la Inspección Jefe del Consejo de Ministros, las inspecciones ministeriales y la Comisión de Lucha contra la Corrupción, que actuó como autoridad central para recibir denuncias de corrupción y conflictos de intereses. Además, algunas instituciones públicas y empresas privadas, en particular las que operan a nivel internacional o en sectores regulados, ya habían desarrollado mecanismos internos de presentación de denuncias.

Este marco fragmentado ayudó a facilitar la transposición de la Directiva a la legislación nacional. En 2023, **Bulgaria** adoptó la Ley de Protección de las Personas que Denuncian o Divulgan Información Pública sobre Infracciones, que entró en vigor el 4 de mayo de 2023. La Ley obliga a los empleadores del sector público y privado con 50 o más empleados a establecer canales internos de denuncia, con la obligación para los empleadores privados con 50-249 empleados a partir del 17 de diciembre de 2023. La Comisión para la Protección de Datos Personales (CPDP), designada como autoridad central para la presentación de denuncias externas, ha tomado desde entonces medidas importantes para implementar y hacer cumplir la legislación.

DENUNCIA DE IRREGULARIDADES EN ESPAÑA

En virtud de la Ley de *Enjuiciamiento Criminal* (LECrim) de 1882, las personas que presencien delitos en **España** están legalmente obligadas a denunciarlos, con las sanciones correspondientes en caso de incumplimiento. Este deber se extiende a los "testigos de referencia" (artículo 264 de la LECrim) y a determinadas profesiones, como las administraciones públicas, que se enfrentan a penas más severas por no denunciar delitos (art. 262 LECrim y 408 del Código Penal español).

Por otro lado, la reforma del Código Penal español de 2015 introdujo el requisito de que los programas de cumplimiento incluyan la obligación de informar "los posibles riesgos e infracciones al órgano responsable de supervisar el funcionamiento y la aplicación del modelo de prevención" (artículo 31 bis 5.4). Aunque el Código Penal no lo incluye como una obligación, en caso de un proceso penal, aquellas entidades que deseen obtener una exención o atenuación de su responsabilidad deben contar con canales internos de denuncia, lo que en la práctica ha hecho que en **España** muchas entidades privadas (especialmente grandes empresas) hayan adoptado estos mecanismos desde antes de la adopción de la Directiva 2019/1937, cada entidad ha desarrollado sus propias políticas y procedimientos de protección de denunciantes sin el amparo de un marco legal claro y común.. En el sector público, también han existido manifestaciones normativas a nivel autonómico previas a la Directiva, por ejemplo, con la Ley 11/2016, de 28 de noviembre, por la que se crea la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana, que impone la obligación de establecer canales confidenciales que garanticen una estricta confidencialidad para la formulación de denuncias cuando el denunciante invoque la aplicación del estatuto regulado en esta Ley.

Sin embargo, es con la transposición de 2019 de la Directiva 2019/1937/UE, efectuada a través de la *Ley 2/2023, de 20 de febrero y 23, reguladora de la protección de las personas que denuncian infracciones normativas y de lucha contra la corrupción* que **España** ha podido contar con un marco de protección universal, generalizada y coherente de las personas informantes.



Transparencia y comunicación en los sistemas de información



Capítulo 1

TRANSPARENCIA Y COMUNICACIÓN DE LOS SISTEMAS DE INFORMACIÓN

Capítulo 1

1.1 UNA APROXIMACIÓN AL PRINCIPIO DE TRANSPARENCIA EN SISTEMAS DE INFORMACIÓN

La confianza³ en el sistema es un factor clave para cualquier informante. La falta de información adecuada sobre los canales disponibles puede tener un impacto directo en el nivel de confianza, y en última instancia afectar al entorno de apoyo y protección para las personas que informen sobre irregularidades. Así, transparencia, confianza y eficacia se posicionan como una unidad trimembre estrechamente vinculada para la consecución de los fines de la normativa de protección de informantes.

De este modo, la ausencia de directrices claras puede dar lugar a desinformación o desconfianza, desalentando a las personas informantes y obstaculizando la creación de un espacio seguro para denunciar las infracciones. Por lo tanto, para **aumentar la confianza y la concienciación**, es necesario **proporcionar información**, como mínimo, sobre:

- A. Quién puede o debe denunciar
- B. Cómo se puede denunciar
- C. Cuándo se debe denunciar
- D. Qué órganos pueden gestionar las comunicaciones
- E. Derechos de las personas informantes
- F. Derechos de las personas investigadas
- G. Cómo se protege a las personas informantes
- H. Principios esenciales del sistema y el procedimiento
- I. Las medidas de seguridad implementadas
- J. Cómo garantizar que el sistema de presentación de denuncias incorpora un enfoque de género

Según una consulta pública realizada en 2017, **solo el 15% de los ciudadanos conocía** las normas vigentes de protección de los denunciantes, y **el 49% no sabía dónde denunciar la corrupción** u otras conductas fraudulentas (UE, 2018)⁴. Del mismo modo, algunos estudios⁵ han demostrado que establecer una base sólida para un programa de denuncia de irregularidades, es decir, definir procedimientos operativos claros o directrices tanto para los funcionarios y miembros del personal de las autoridades como para las personas informantes, es una práctica eficaz para gestionar adecuadamente la confianza hacia las entidades y la revelación de

³ Según Binikos (2008), la confianza en las entidades y en los canales de denuncia se asoció positivamente con las intenciones de denunciar en 16 estudios (entre otros: Attree, 2007; Brennan y Kelly, 2007; Binikos, 2008; Curtis y Taylor, 2009; Seifert et al., 2014; etc.).

⁴ Ver: <https://ec.europa.eu/newsroom/just/items/54254/en>

⁵ Comisión Australiana de Valores e Inversiones, 2023; entre otros.

información. Debido a que la denuncia de irregularidades es un proceso complejo con implicaciones personales y psicológicas, se requieren medidas organizativas y culturales para apoyar la implementación de la ley, al tiempo que se deben tener en cuenta los aspectos culturales hacia las personas informantes⁶.

A pesar de que la Directiva define claramente **los derechos y principios**, no contiene disposiciones claras y detalladas sobre la información y la transparencia que todas las entidades obligadas (artículo 8) deben proporcionar públicamente sobre los elementos esenciales de sus **canales y sistemas**. De esta forma, el artículo 13 de la Directiva establece una obligación general para las autoridades competentes, mientras que el artículo 9.1 impone a las entidades obligadas la obligación de informar sobre los "procedimientos de notificación externa a las autoridades competentes de conformidad con el artículo 10 y, en su caso, a las instituciones, órganos u organismos de la Unión" (art. 9.1.(g)).

Esta falta de concreción y desarrollo puede llevar a que **los y las posibles informantes** puedan no contar con toda la información necesaria sobre los canales disponibles, el sistema de denuncia, los procedimientos y autoridades involucrados, los derechos, los plazos, la información técnica, las medidas de protección y las características del sistema de seguridad informática.

En **España**, la Ley 2/2023, de 20 de febrero, de 23 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción⁷, dedica el Título IV a regular la información que deben facilitar tanto las entidades como las autoridades competentes en los canales internos y externos. La ley estipula expresamente que esta información **debe ser visible en sitios web** o plataformas electrónicas, en una sección separada y de fácil acceso. También exige que todas las entidades que deban tener un canal interno, tanto en el sector público como en el privado, lleven un libro de registro de las denuncias recibidas y de las investigaciones internas que se deriven de ellas. Sin embargo, este libro de registro no es público y solo es accesible para las autoridades judiciales.

El artículo 25 de la Ley 2/23 establece explícitamente que: " Los sujetos comprendidos dentro del ámbito de aplicación de esta ley proporcionarán la información adecuada de forma clara y fácilmente accesible, sobre el uso de todo canal interno de información que hayan implantado, así como sobre los principios esenciales del procedimiento de gestión. En caso de contar con una página web, dicha información deberá constar en la página de inicio, en una sección separada y fácilmente identificable". Sin embargo, la ley no especifica el contenido esencial de lo que las entidades deben informar necesariamente al público sobre sus sistemas de información en sus sitios web⁸. Esta omisión puede generar interpretaciones diversas entre

⁶ Teichmann et al., 2022.

⁷ Ley 2/2023, de 20 de febrero, de 23 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción <https://www.boe.es/buscar/act.php?id=BOE-A-2023-4513>

⁸ Para las autoridades mencionadas en el artículo 24, la Ley arroja un poco más de luz al establecer que deberán publicar, en una sección separada, fácilmente identificable y accesible de su sitio electrónico, al menos, la siguiente información: "a) las condiciones de elegibilidad para la protección prevista en la presente ley; b) los datos de contacto de los canales de información externos previstos en el título III, en particular, las direcciones de correo electrónico y postal y los números de teléfono asociados a dichos canales, indicando si las conversaciones telefónicas están grabadas; c) los procedimientos de gestión, incluida la forma en que la autoridad competente podrá solicitar al informante que aclare la información comunicada o que facilite información adicional, el plazo para responder al informante, en su caso, y el tipo y contenido de dicha respuesta; d) el régimen de confidencialidad aplicable a las comunicaciones y, en particular, a la información sobre el tratamiento de datos personales de conformidad con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Ley Orgánica 3/2018, de 5 de diciembre, y el Título VII de la presente ley. e) recursos y procedimientos para la protección contra represalias, y la disponibilidad de asesoramiento confidencial. En particular, se establecerán las condiciones para la exención de responsabilidad y la atenuación de la sanción a que se refiere el artículo 40 y f) los datos de contacto de la Autoridad Independiente de Protección de los Denunciantes, I.W.P.A. o de la autoridad u organismo competente de que se trate.».

las organizaciones, lo que podría afectar la uniformidad, la eficacia y la transparencia en la implementación de los canales internos de información.

En **Italia**, todas las entidades, tanto del sector público como del privado, tienen la obligación de **proporcionar información clara, detallada y fácilmente accesible sobre los canales** habilitados para la presentación de denuncias, tanto internos como externos, así como sobre los procedimientos aplicables y los requisitos previos que deben cumplirse para su correcta tramitación⁹.

Esta información **debe ser fácilmente visible en el lugar de trabajo** y accesible para las personas con una relación jurídica con la entidad. Si la entidad tiene un sitio web, la información debe publicarse en una sección específica. Adicionalmente, la Ley¹⁰ establece que, como **autoridad competente** para gestionar el canal de denuncia externo, la Autoridad Nacional Anticorrupción (ANAC) debe publicar información como:

- A. Medidas de protección para los denunciantes.
- B. Datos de contacto, como el número de teléfono de la oficina o canal externo que gestiona las denuncias, indicando si las conversaciones telefónicas están grabadas o no, la dirección postal y la dirección de correo electrónico, tanto ordinaria como certificada.
- C. Normas de confidencialidad aplicables a las denuncias externas e internas.

En **Bulgaria**, la *Ley de Protección de las Personas que Denuncian públicamente Información sobre Infracciones*, de 4 de mayo de 2023, en consonancia con la Directiva, establece que "(...) Las entidades obligadas facilitarán información clara y fácilmente accesible sobre las condiciones y procedimientos para la presentación de denuncias de irregularidades. La información se publicará en los sitios web de las entidades obligadas, así como en lugares destacados de las oficinas y lugares de trabajo"¹¹ (artículo 12, apartado 4).». Aunque esta obligación se ha **aplicado formalmente, no se ha evaluado su eficacia**.

La transparencia significativa y la comunicación efectiva no son cuestiones menores, sino esenciales para garantizar el correcto funcionamiento de los sistemas de denuncia de irregularidades. Las personas no pueden tomar decisiones informadas sobre si, cuándo y cómo denunciar si no están adecuadamente informadas con antelación sobre sus **derechos y obligaciones fundamentales**, los **principios** y **pasos esenciales del proceso de denuncia** y los detalles básicos sobre la naturaleza y el funcionamiento de los canales de denuncia dentro de una organización u organismo público¹².

⁹ Art.51 Decreto Legislativo, 10 de marzo de 2023, n.24

¹⁰ Art. 9 del Decreto Legislativo 24/2023, por el que se transpone la Directiva 2019/1937/UE

¹¹ Ley de Protección de las Personas que Denuncian o Divulgan Información Pública sobre Infracciones, Bulgaria, 4 de mayo de 2023, artículo 12(4)

¹² El legislador europeo ha sido muy claro en este sentido: "todas las personas que se planteen denunciar infracciones del Derecho de la Unión deberían poder tomar una decisión informada sobre si, cuándo y cómo denunciar. Las personas jurídicas de los sectores público y privado que cuenten con procedimientos internos de presentación de denuncias deben proporcionar información sobre estos procedimientos, así como sobre los procedimientos de presentación de denuncias externas a las autoridades competentes. Es esencial que esta información sea clara y de fácil acceso, incluso, en la medida de lo posible, a las personas que no son empleados en contacto con la entidad debido a sus actividades profesionales, como proveedores de servicios, distribuidores, proveedores y socios comerciales. Por ejemplo, dicha información podría mostrarse en un lugar visible accesible para todas estas personas y en el sitio web de la entidad, y también podría incluirse en cursos y seminarios de capacitación en ética e integridad". (Considerando 59 de la Directiva 2019/1937/UE). Además, en un considerando posterior, se reitera que "toda la información relativa a las denuncias debe ser transparente, fácilmente comprensible y fiable a fin de fomentar la denuncia en lugar de obstaculirla". (Considerando 75 de la Directiva 2019/1937/UE).

Asimismo, las autoridades y órganos de supervisión pueden **ejercer un control más efectivo** sobre las entidades obligadas mediante la realización de revisiones periódicas del cumplimiento de las medidas de transparencia, así como fomentando activamente la implementación de canales de denuncia accesibles y eficaces.

De los Considerandos núm. 59 y 75 de la Directiva, junto con los artículo 25 de la Ley 2/23 española, 12 de la Ley de Protección al Denunciante de Irregularidades de **Bulgaria**, y 5.1 y 9.1 del Decreto Legislativo italiano 24/2023, se desprende, en consecuencia, que existen dos condiciones básicas que deben necesariamente cumplirse para garantizar una transparencia adecuada e integral de los sistemas y canales de información y que estos así puedan cumplir adecuadamente su misión: **una de fondo y otra de forma**.

1.2 TRANSPARENCIA DE LOS SISTEMAS Y CANALES DE INFORMACIÓN: REQUISITOS DE FONDO.

En cuanto al aspecto sustantivo, todos los sujetos obligados deberán proporcionar **información clara, completa, actualizada y estructurada**, al menos, sobre las siguientes materias:

1.2.1 TRANSPARENCIA RESPECTO A LOS DERECHOS Y GARANTÍAS DE LAS PERSONAS INFORMANTES Y PERSONAS AFECTADAS

Es necesario incluir un apartado específico (tanto en la web como en la intranet, si procede) con una lista completa de **los derechos tanto de las personas informantes como de las personas afectadas**, así como de terceros (por ejemplo, alguien que se menciona en la denuncia, testigos, representantes/sindicatos de los trabajadores, compañeros de trabajo, etc).

En cuanto a los derechos de las personas informantes, es preciso incluir al menos los siguientes:

- A. Protección de la confidencialidad de las personas informantes y del contenido de la denuncia.
- B. No represalias¹³ en los términos establecidos en la Directiva y en las legislaciones nacionales.
- C. Información clara sobre los órganos que reciben, gestionan e instruyen las denuncias.
- D. Derecho a recibir una respuesta motivada sobre la decisión de archivar, desestimar o no proceder con la denuncia.
- E. Protección de datos personales¹⁴.
- F. Acuse de recibo y seguimiento diligente de las denuncias.
- G. Notificación de resolución oportuna y adecuada¹⁵.
- H. Una investigación justa, independiente e imparcial.

¹³ Según uno de los expertos entrevistados, es importante informar sobre cómo se evitan las represalias, cómo se garantiza la protección de los denunciantes y describir los procesos específicos que lo garantizan.

¹⁴ A título enunciativo y no limitativo: el derecho a ser informado sobre la identidad del responsable del tratamiento, la finalidad del tratamiento y la posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del RGPD y el derecho a la supresión de los datos después de tres meses, a menos que se inicien procedimientos disciplinarios o penales disciplinarios o penales.

¹⁵ A este respecto, véase. Indicador n° 94 del Informe TRAC-ESPAÑA 2022 (p. 159).

- I. Asesoramiento jurídico, apoyo jurídico y psicológico, o apoyo de los representantes de los trabajadores. (si así lo exige la ley).
- J. Derecho a una buena administración, en virtud del artículo 41 de la Carta de los Derechos Fundamentales de la Unión Europea (especialmente relevante para las entidades obligadas del sector público).
- K. Apoyo psicológico (si así lo exige la ley u ofrecido por la entidad).
- L. Apoyo financiero (si así lo exige la ley u ofrecido por la entidad).

En cuanto a los derechos de las personas afectadas, es preciso incluir al menos los siguientes:

- A. Presunción de inocencia.
- B. Protección de la identidad/confidencialidad.
- C. Derecho a ser oído.
- D. Acceso al expediente de investigación.
- E. Derecho al debido proceso.
- F. Derecho a presentar pruebas.
- G. Defensa legal y representación de los trabajadores.
- H. Derecho a conocer al órgano instructor y a un juez imparcial.
- I. Derechos de protección de datos personales.

Por último, resulta importante incluir una referencia explícita a los **derechos y garantías de terceros** que puedan estar relacionados, directa o indirectamente, con una denuncia. Esto incluye a personas mencionadas en el informe, testigos, familiares, o cualquier otra persona que pudiera verse afectada, sufrir represalias o daño como consecuencia del procedimiento, así como a quienes brinden apoyo legal, psicológico o laboral a la persona informante.

Asimismo, debe contemplarse la protección de los **centros de apoyo a informantes** e incluir información específica sobre su papel y garantías, conforme se detalla en el [Capítulo 4](#) del documento.

CP. 4 ➔

1.2.2 TRANSPARENCIA SOBRE EL ALCANCE MATERIAL DE LA PRESENTACIÓN DE DENUNCIAS

Es recomendable indicar cuál es el ámbito en el que se puede denunciar, así como la normativa aplicable¹⁶. Además, se recomienda que los canales internos y externos proporcionen un punto de contacto para consultas y una sección de preguntas frecuentes.

Varios expertos entrevistados en el marco del proyecto OPWHI han señalado que algunas de las leyes por las que se ha transpuesto la Directiva 2019/1937 algunas han dejado ambigüedades, desigualdades o zonas desprotegidas en varios aspectos, y entre ellos: qué puede o no¹⁷ ser susceptible de comunicación o denuncia. Estas áreas desprotegidas pueden desalentar a

¹⁶ De hecho, otro de nuestros entrevistados destacó que es crucial estar informado sobre el marco legal y el riesgo de litigios.

¹⁷ Por ejemplo, en España, la Ley 2/2023 solo protege y reconoce derechos a quienes informen únicamente sobre: a) infracciones penales (delitos), b) infracciones administrativas graves o muy graves y/o c) infracciones del Derecho de la Unión Europea y que afecten a los intereses financieros de la Unión Europea; excluyendo, por ejemplo, delitos menores o casos que podrían ayudar a prevenir delitos más graves. Algunos de los expertos también plantearon la cuestión de si se aceptarían las denuncias de mala administración.

los posibles informantes. Por ejemplo, según la Ley 2/2023 en **España**, las personas informantes que denuncien irregularidades que impliquen un delito leve en materias distintas a las contenidas en la Directiva no tendrían derecho a su protección.

PERSPECTIVA DE GÉNERO

Todos los expertos entrevistados en el marco del proyecto han hecho hincapié en la necesidad de abordar las desigualdades intersectoriales e interseccionales, incorporando la perspectiva de género y diversidad. La falta de información, así como el riesgo asociado, influyen significativamente en la decisión de denunciar.

Según estos expertos, los casos de abusos de poder por motivos de género, como el acoso sexual o la sextorsión, suelen estar relacionados con un mayor riesgo de represalias (**véase el recuadro del capítulo 4**), lo que puede disuadir a las víctimas de denunciar. En algunos casos, las víctimas pueden no estar seguras de si tales conductas indebidas entran en el ámbito de aplicación de la legislación sobre denuncias de irregularidades. Las partes interesadas han recomendado incluir explícitamente estas cuestiones en los marcos de denuncia de irregularidades. En **Bulgaria**, los representantes de la sociedad civil han hecho hincapié en que, si surgen problemas relacionados con el género en el lugar de trabajo, la legislación sobre denuncias de irregularidades debe abordarlos junto con las disposiciones legales existentes contra la discriminación.

Se recomienda, por tanto:

- A. Garantizar que la legislación de la UE sobre violencia de género y las normas nacionales se integren en los mecanismos de denuncia de irregularidades para proporcionar una protección integral.
- B. Ampliar el alcance de la protección para cubrir todas las posibles irregularidades, abusos y otros delitos, incluidos el acoso sexual y la sextorsión. El marco jurídico de la denuncia de irregularidades debe abordar la discriminación de género en el lugar de trabajo, además de las disposiciones legales aplicables contra la discriminación, y proporcionar apoyo y protección a las víctimas de sextorsión y acoso sexual en el marco de la legislación en materia de denuncia de irregularidades.
- C. Reforzar las medidas para establecer mecanismos de protección adaptados para las mujeres denunciantes y otros grupos vulnerables a través de futuros marcos regulatorios internacionales, nacionales y subnacionales, garantizando que los canales de denuncia sean accesibles, inclusivos y respondan a sus necesidades y riesgos específicos.
- D. Desarrollar protocolos sensibles al género dentro de los marcos de denuncia de irregularidades para abordar específicamente los casos de acoso sexual, sextorsión y otras conductas indebidas basadas en el género. Integrar la transparencia con respecto a los derechos y salvaguardas de las personas informantes, con énfasis en la comunicación sensible al género y la inclusión de grupos marginados. Una comunicación clara sobre los derechos, las garantías y las autoridades responsables de tramitar las denuncias garantiza que las personas informantes se sientan seguros en el sistema y comprendan sus protecciones. Esto incluye pautas claras y accesibles sobre los procedimientos, las opciones de apoyo y las protecciones legales contra las represalias.
- E. Garantizar una coordinación interinstitucional efectiva para un manejo más eficaz y prevenir la impunidad, evitando la suposición de que los casos de sextorsión pueden abordarse mejor con otros servicios o mecanismos de denuncia, como los que se ocupan de la violencia sexual.
- F. Proporcionar ejemplos concretos de casos basados en el género para mejorar la claridad y la accesibilidad para los posibles informantes, reforzando sus derechos y las protecciones disponibles.
- G. Asegurar que cada persona deba ser informada de su derecho a denunciar o revelar irregularidades directamente a las autoridades especializadas pertinentes, como la policía, la fiscalía o los tribunales, en particular en casos de violencia de género. Esto garantiza que la persona esté al tanto de todas las opciones disponibles para abordar el problema y busque el apoyo adecuado. Los acuerdos de compensación no deben excluir el acceso a los sistemas de justicia.

- # Garantizar que las plataformas de denuncia utilicen un lenguaje claro y no técnico y ofrezcan canales en varios idiomas, incluido el lenguaje de señas y otros formatos accesibles, para dar cabida a una amplia gama de informantes. Garantizar un lenguaje inclusivo de género, visibilizando el género cuando sea pertinente y evitando marcadores de género innecesarios cuando no sean pertinentes para la comunicación. Este enfoque promueve la claridad, la inclusión y el respeto por las diversas identidades de género en todas las formas de comunicación.
- I. Considerar el impacto de las disparidades en el acceso digital, garantizando mecanismos alternativos de denuncia fuera de línea para las personas sin acceso seguro a Internet, promoviendo la inclusión para todos los usuarios, independientemente de sus capacidades de acceso digital.

QUÉ OCURRE EN LAS LEGISLACIONES NACIONALES

ITALIA

El concepto de acoso sexual es pertinente desde el punto de vista de la legislación contra la discriminación desde 2006, cuando se adopta el llamado Código de Igualdad de Oportunidades para Hombres y Mujeres (Decreto Legislativo n.º 198/2006). En ausencia de una legislación sobre denuncias de irregularidades que abarque el acoso sexual en el trabajo, se deja a la voluntad de los empleadores aplicar procedimientos internos que permitan a los empleados denunciar el acoso o la intimidación.

ESPAÑA

La Ley 2/2023 no aborda explícitamente la violencia de género. Sin embargo, opera dentro de un marco normativo reconocido para la prevención de la violencia de género, la igualdad y la no discriminación, así como de planes nacionales y políticas públicas específicas en esta materia. Vale la pena mencionar tres puntos clave:

- A. El ámbito de aplicación material de la ley va más allá de los requisitos europeos y se aplica tanto a las infracciones penales como a las administrativas graves y muy graves, incluidas las violaciones de la legislación nacional. Esto permite que los mecanismos de denuncia incluyan todos los delitos de violencia de género⁴⁰.
- B. A pesar de que la ley no impide incorporar esta cuestión en normativas o protocolos, la protección basada en el género es plenamente compatible con el marco legal de la denuncia de irregularidades. No solo ambos deben integrarse en el marco legal de la violencia de género, sino que la ley de denuncia de irregularidades también incluye protecciones para los trabajadores que denuncian cualquier forma de abuso o violaciones de su dignidad, salud y seguridad. Por lo tanto, la protección y salvaguarda deben cubrir cualquier violación de la integridad física o psicológica, incluida cualquier forma de discriminación de género o abuso sexual.
- C. El Real Decreto por el que se crea la Autoridad Independiente para la Protección de los Informantes (A.A.I.) exige una representación equilibrada de género en la Comisión Consultiva, sentando un valioso precedente para otras autoridades nacionales o locales.

⁴⁰ A este respecto, vid Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual.

BULGARIA

El acoso sexual no está contemplado en la Ley Nacional de Denuncia de Irregularidades. Sin embargo, diversas entidades búlgaras incorporan situaciones donde, si el acoso se produce en un contexto laboral y amenaza el interés público, la denuncia podría considerarse una denuncia de irregularidades, y la persona informante podría recibir la debida protección.

1.2.3 TRANSPARENCIA EN CUANTO A LOS PRINCIPIOS ESENCIALES¹⁸ DEL PROCEDIMIENTO DE GESTIÓN, SEGURIDAD, INDEMNIDAD, CONFIDENCIALIDAD Y ANONIMATO.

Las entidades **deben definir claramente** los principios esenciales del procedimiento de denuncia de irregularidades, incluido su propósito, gestión y marco de cumplimiento. Por ejemplo, en **España**, estos principios deben quedar reflejados explícitamente en la Política del Sistema Interno de Información (art. 5.2. h) Ley 2/23). Brindar información adecuada en esta sección será clave ya que permitirá informar debidamente sobre cuáles son los motivos de existencia del canal y sus fines concretos, incentivando así un uso correcto del mismo y desincentivando, en consecuencia, un uso indebido.

Asimismo, se debe informar necesariamente sobre cuatro elementos fundamentales del sistema:

- A. En cuanto a la **seguridad**, es esencial informar sobre las características informáticas del servidor o la plataforma y las medidas de seguridad de la información adoptadas para garantizar un entorno digital seguro para las personas informantes, a saber: cifrado, seudonimización, codificación, cajas negras, control de acceso, protocolos de conexión segura, autenticación en dos etapas, reglas de validación, descripciones adecuadas de los cortafuegos, descripciones exhaustivas de las características del servidor/software, Token CSRF, etc.
- B. En relación con la indemnidad, es necesario informar de manera clara sobre el alcance de la protección de las personas informantes, las condiciones para acceder a la protección en virtud de la Ley y garantizar explícitamente que no habrá represalias contra las personas informantes si las denuncias son fundadas. Es importante destacar que la protección debe garantizarse incluso si una denuncia no está fundada, pero la persona informante creyó razonablemente que era cierta.
- C. En cuanto a la **confidencialidad**, debe explicarse de forma clara y sencilla cómo se garantiza la confidencialidad de la persona informante, a saber: garantía del principio de acceso mínimo e integridad de los datos, explicación/justificación del tratamiento de datos, descripción del tratamiento de datos durante todas las fases del proceso, tiempo de conservación y ubicación de la información, medidas de protección de los datos y de la identidad de la persona informante, descripción de los sistemas de anonimización y/o seudonimización, descripción del control, la supervisión y segregación de los expedientes de los y las informantes, medidas para evitar la reidentificación, etc.; Y en caso de que el canal o una parte del proceso esté externalizado, es importante describir todas las medidas de seguridad establecidas por el proveedor y el servidor.
- D. Sobre el **anonimato**, es fundamental que los canales de denuncia estén diseñados de forma que permitan, si así lo desea el informante, presentar comunicaciones de manera completamente anónima. No obstante, conviene subrayar que la Directiva no reconoce el anonimato como una garantía obligatoria, sino que deja a los Estados miembros la posibilidad de admitir y tramitar denuncias anónimas según su legislación nacional. Por tanto, aunque el anonimato no está garantizado directamente por la Directiva, su incorporación voluntaria en los sistemas de denuncia constituye una buena práctica.

¹⁸ Artículo 5.2. h) Ley 2/23 española, art 13 Ley búlgara, art. 4, 5, 7, 8 del Decreto Legislativo italiano 24/2023, de transposición de la Directiva 2019/1937/UE.

En cuanto a las características elementales sobre la confidencialidad y anonimato: Si la persona informante se identifica en el canal o sistema, la **confidencialidad** garantiza que su identidad no sea revelada a personas no autorizadas. Los sistemas de seguridad (generalmente logrados a través de encriptación, controles de acceso, etc.) podrían ser útiles para mantener la confidencialidad protegida, pero es necesario desarrollar políticas internas de denuncia de irregularidades que detallen el régimen de confidencialidad y las funciones de las personas responsables para garantizar que la identidad de las personas informantes permanezca protegida.

El **anonimato**, por su parte, debe garantizar que una persona que quiera mantener su identidad en secreto pueda estar segura de que este es el caso, por lo tanto, en este caso, la identidad de una persona no podría en ningún modo vincularse a sus acciones, visualizaciones, datos o propiedad intelectual, protegiendo la falta de trazabilidad de la identidad de la persona informante (logrado, por ejemplo, a través de sistemas TOR o pruebas de conocimiento cero).

Según la opinión de algunos expertos entrevistados en el marco del proyecto, se han detectado una serie de buzones o canales de algunas instituciones públicas¹⁹ que dicen garantizar el anonimato, pero en la práctica no es así.

1.2.4 ÓRGANOS DE RECEPCIÓN, GESTIÓN, INVESTIGACIÓN Y RESOLUCIÓN

Es importante garantizar la transparencia con respecto al **órgano receptor** y al **órgano de gestión** (en caso de estar separados), así como al **órgano de investigación** y **órgano de resolución**. Esta separación orgánica es crucial no solo para fomentar una mayor confianza en el sistema, sino también para garantizar el cumplimiento del principio de imparcialidad e independencia en todos los procesos de investigación iniciados como resultado de las denuncias.

También es necesario incluir **una explicación de las medidas** implementadas para prevenir posibles **conflictos de interés** entre los organismos o diferentes departamentos y proporcionar opciones alternativas si la persona responsable del sistema o cualquier miembro de los organismos intervinientes (órganos receptores, gerentes, instructores o resolutores, así como segundas instancias o posibles instancias) están involucrados en el informe.

¹⁹ A este respecto, véase: <https://xnet-x.net/es/proliferacion-buzones-anonimos-no-lo-son/>

1.2.5. TRANSPARENCIA SOBRE PLAZOS DE ACUSE, ADMISIÓN, INVESTIGACIÓN Y RESOLUCIÓN

1) Plazo de accuse de recibo

De acuerdo con la Directiva (art. 9.2²⁰), el **acuse de recibo** debe darse a la persona informante en un plazo máximo de siete días naturales a partir de la recepción o registro de la denuncia, a menos que ello pueda poner en peligro la confidencialidad.

2) Plazos de admisión

El sitio web o intranet debe indicar el plazo de admisión de la denuncia en caso de superar el análisis preliminar de **admisibilidad**²¹ o si por el contrario debe procederse a su archivo. En consecuencia, la entidad debe informar explícitamente sobre los siguientes aspectos:

- A. **Plazo máximo para la realización de la prueba preliminar de admisibilidad a fin de evitar demoras indebidas.** Ni la Directiva 2019/1937, ni la Ley 2/2023, ni las legislaciones de **Bulgaria** o **Italia** establecen de forma expresa un plazo general para la tramitación inicial de las denuncias. No obstante, la Ley 2/2023 sí fija un plazo específico para la Autoridad Independiente de Protección del Informante (A.A.I.) en **España**, estableciendo que la admisión o archivo de una denuncia debe producirse en un plazo no superior a “diez días hábiles” desde la fecha de registro de la comunicación. Este puede constituir un parámetro útil de referencia, adaptable según las características y capacidades de cada entidad. En cualquier caso, se recomienda que las organizaciones establezcan y publiquen un marco temporal claro y transparente sobre la gestión de sus denuncias, con el fin de evitar dilaciones indebidas y reforzar la confianza en el sistema.
- B. **Plazo máximo para comunicar a la persona informante sobre la admisión a trámite o archivo de la denuncia/comunicación.** De nuevo, ni la Directiva 2019/1937 ni la ley española, búlgara o italiana regulan claramente este aspecto. Por ejemplo, la Ley española establece un plazo máximo de notificación de “cinco días hábiles”, pero no especifica desde cuándo deben contarse estos cinco días.

En nuestra opinión, este **plazo debería comenzar a contar desde** el momento en que se ejecuta la prueba preliminar de admisibilidad (cuyo plazo máximo de ejecución, como se indicó anteriormente, sería por ejemplo de diez días hábiles a partir de la fecha de registro²²), a menos que, conforme al artículo 17.4 de la Ley 2/23 la denuncia sea anónima o la persona informante haya renunciado a recibir notificaciones.

Otro aspecto relevante a considerar es que, de acuerdo con la Ley 2/2023, los plazos establecidos para la tramitación y presentación de denuncias se refieren exclusivamente a la persona informante, sin contemplar

²⁰ Art. 9.2c) de la Ley 2/23; art. 5.2. Par. h) de la Ley búlgara; art.5 a) y 7.3 de la Ley italiana, respectivamente para los canales internos y externos, estableciendo también un plazo de 7 días para emitir un recibo de la denuncia.

²¹ Al respecto, véase MARTÍNEZ GARCÍA, D (2021). «Anonimato, seudónimo y confidencialidad: hacia un marco integral y coherente para la protección de los denunciantes»

²² Por ejemplo, si la prueba de admisibilidad se completa al octavo día hábil después del registro de la comunicación, la entidad tendría cinco días hábiles adicionales a partir de ese momento para notificar al denunciante si su comunicación es admitida, haciendo un total de trece días hábiles desde el registro de la comunicación.

expresamente plazos ni procedimientos de notificación para la persona afectada durante esta fase inicial. Tanto la Directiva europea como las legislaciones nacionales —incluida la española— omiten establecer plazos claros para informar a la persona presuntamente implicada en los hechos denunciados, especialmente en los casos en que la denuncia no supera la evaluación preliminar de admisibilidad. Esta laguna normativa plantea interrogantes importantes en términos de garantías procesales, como el derecho a la información y el principio de contradicción, y subraya la necesidad de clarificar si la persona afectada debe ser notificada incluso cuando el informe es archivado sin mayores actuaciones. A falta de una regulación explícita, se corre el riesgo de generar incertidumbre jurídica y afectar la confianza en el sistema de denuncias internas.

Sobre la notificación a la persona afectada sobre el archivo de una denuncia que no superó el test de admisibilidad, se podría colegir, de una lectura amplia del artículo 18.2.a) 4º de la Ley 2/2023, que dicha notificación no sería necesaria ya que establece la inadmisibilidad por falta de **información nueva o significativa** respecto a una comunicación anterior “respecto de la cual han concluido los correspondientes procedimientos”.

Sin embargo, se trata de una fórmula procesalmente ambigua ya que:

- A. Al hablar de procedimientos en plural, se puede referir a una comunicación archivada²³ por no haber superado el **test de admisibilidad** y que posteriormente con una nueva comunicación complementaria se logre aportar esta vez información relevante, significativa o nuevas evidencias determinantes²⁴; cuestión que, a su vez, puede plantear la problemática (no resulta por la Ley) del tiempo máximo de conservación de datos personales de una denuncia archivada, ya que, por ejemplo, a tenor de lo dispuesto en el artículo 32.3, si la denuncia se inadmite por la causa establecida en el art. 18.2 a) 1º, es decir, por carencia de verosimilitud, si se acreditase que la información facilitada o parte de ella no es veraz, de acuerdo con la Ley, “deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial”, y, en todo caso, no más de tres meses, salvo que la finalidad de la conservación sea dejar precisamente evidencia del funcionamiento del sistema²⁵, debiendo conservar la información siempre, además, de manera anonimizada.
- B. Se puede referir a casos donde, tras haberse decretado la no notificación a la persona afectada hasta la fase de audiencia por riesgo de posible destrucción, ocultación o alteración de pruebas (art. 19.2 de la Ley 2/23) se produzcan comunicaciones complementarias (en el marco del art. 18.2 a) 4º) por parte de la persona informante e incluyendo acusaciones nuevas sobre la persona informante y que a priori, salvo una vez más riesgo de ocultación, destrucción o alteración de evidencias vinculadas a estas nuevas acusaciones, se le debería notificar a la persona afectada según el procedimiento habitual para de este modo evitar una posible indefensión.

²³ Toda notificación sobre el archivo de una denuncia debe hacerse de forma suficientemente motivada.

²⁴ Siempre y cuando estas nuevas evidencias no hayan sido recabadas vulnerando derechos o libertades fundamentales o de forma ilegal.

²⁵ Lo que puede plantear problemas sobre una ilimitada potencial reapertura de casos archivados en fase de la evaluación preliminar, lo que plantea cuestionamientos vinculados a la posible conculcación del principio non bis in idem.

3) Plazos del proceso de investigación

Si bien la normativa española establece expresamente que “se garantizará que la persona afectada por la información tenga noticia de la misma, así como de los hechos relatados de manera sucinta”, no se establece sin embargo un plazo claro para ello, por lo que serán las entidades las que determinen en sus políticas internas dichos plazos para garantizar la protección de los derechos procesales de la persona afectada y en todo caso un adecuado derecho a ser informado de los hechos que se le atribuyan, así como de cualquier cambio relevante en el objeto de la investigación y de los hechos imputados (art. 118.1 a) LECrim).

A este respecto, la Ley de Enjuiciamiento Criminal es muy clara en cuanto a que “esta información será facilitada con el grado de detalle suficiente para permitir el ejercicio efectivo del derecho de defensa”, lo que invita a pensar que para asegurar una protección adecuada de este derecho es necesario garantizar un grado de detalle suficiente y no sólo un relato sucinto de los hechos. Los autores de la presente guía consideramos que una vez acordada la admisión a trámite se le debería otorgar el mismo plazo máximo de notificación previsto para la persona informante (y en todo caso nunca un plazo mayor), es decir, cinco días hábiles siguientes a la resolución de admisión a trámite, para notificarle que se acordó admitir a trámite una denuncia de la cual es persona afectada²⁶, salvo que, a juicio del órgano instructor, existan indicios de que puede con la notificación a la persona afectada existir un riesgo elevado para ocultación, destrucción o alteración de las pruebas por parte de la misma o de terceros, en cuyo caso, a tenor del artículo 19.2 de la Ley 2/2023, “esta información podrá efectuarse en el trámite de audiencia”²⁷.

4) Plazo de resolución

En cuanto a los plazos de resolución y de finalización de las actuaciones, se deberá comunicar de forma clara y transparente que el plazo máximo de respuesta²⁸, no excederá de tres meses desde la recepción de la comunicación, salvo en los casos de especial complejidad que requieran una prórroga de hasta un máximo de tres meses adicionales.

1.2.6 RÉGIMEN DISCIPLINARIO APLICABLE

La transparencia con respecto a las medidas disciplinarias aplicables y las consecuencias de comunicar deliberadamente información falsa o engañosa debe estar claramente informada. Es necesario informar adecuadamente sobre el propósito final del canal y desalentar su uso incorrecto.

Con este fin, es aconsejable informar a aquellos que a sabiendas **presentan información falsa**, atribuyendo hechos falsos a otra persona que, de ser ciertos, **constituirían una infracción, o afirmando falsamente ser víctima** de una infracción inexistente. En algunas legislaciones están cometiendo un **delito (art. 456 del Código Penal español) y en otras están sujetas a severas sanciones administrativas (Italia)**.

²⁶ Todo ello con fundamento en el artículo 118.5 LECrim, el cual establece que: “La admisión de denuncia o querrela, y cualquier actuación procesal de la que resulte la imputación de un delito contra persona o personas determinadas, serán puestas inmediatamente en conocimiento de los presuntamente responsables.”

²⁷ Según el artículo 19.2 de la Ley 2/2023 española, el art. 16 de la Ley búlgara.

²⁸ Según el artículo 9.2.d) de la Ley 2/23, art. 16 (para los canales internos) y art. 23 (para el canal externo) de la Ley búlgara; y los art. 5 (relacionados con el canal interno) y 8 (relacionados con el canal externo) de la Ley italiana.

1.2.7. DATOS DE CONTACTO DE LOS CANALES EXTERNOS Y AUTORIDADES COMPETENTES

Es preciso informar siempre sobre los datos de contacto de los **canales oficiales externos**²⁹. Concretamente: las direcciones de correo electrónico y postal y los números de teléfono asociados a estos canales y, en cualquier caso, los datos de contacto de la autoridad independiente³⁰ y otras autoridades competentes para recibir dichas comunicaciones, así como las vías de recurso disponibles y los procedimientos de protección contra represalias, junto con las condiciones para obtener asistencia legal, asesoramiento y apoyo laboral, psicológico y financiero (en caso de que estén previstos).

PERSPECTIVA DE GOBIERNO ABIERTO

Los expertos consultados durante la fase de entrevistas sugieren que **un enfoque colaborativo** que involucre a las Organizaciones de la Sociedad Civil (OSC) y las autoridades públicas **puede mejorar las páginas web y la información sobre los sistemas de denuncias, al tiempo que garantiza una perspectiva orientada a garantizar plena accesibilidad a los canales y al entendimiento por parte de potenciales informantes sobre sus derechos.**

En línea con esto, las organizaciones de la sociedad civil sugieren estrategias simples pero efectivas para mejorar la usabilidad del contenido y aumentar la confianza en los canales de denuncia:

- A. Utilice un lenguaje sencillo que sea fácil de entender, evitando la jerga técnica o legal.
- B. Proporcione ejemplos prácticos siempre que sea posible.
- C. Repita las instrucciones clave de presentación de denuncias a lo largo del proceso de presentación de denuncias, incluso en la página de información y dentro del canal de denuncias.
- D. En la plataforma o formulario de denuncia, solicite primero el asunto de la denuncia y solo pida el nombre de la persona denunciante al final.

Para mejorar los sistemas de presentación de denuncias y las páginas de información, **las consultas públicas abiertas a todas las partes interesadas pueden ayudar a perfeccionar el contenido y la facilidad de uso**, al tiempo que fomentan la presentación de denuncias. La autoridad competente debe liderar dichas consultas, dando ejemplo a otras entidades obligadas para que reproduzcan estos esfuerzos o promuevan sus propias consultas públicas.

Las mejores prácticas en gobierno abierto (OG por sus siglas en inglés) incluyen **proporcionar información clara en los sitios web de las autoridades públicas sobre el apoyo a las personas informantes es y los servicios de asesoramiento** gestionados por instituciones (por ejemplo, la Oficina del Defensor del Pueblo) y OSC. Esta disposición no está contemplada explícitamente en la Directiva. Sin embargo, dado que solo establece normas mínimas, se recomienda encarecidamente a los países de la UE que deseen ir más allá de sus requisitos e incluir esta disposición en sus leyes o reglamentos nacionales que lo hagan.

²⁹ Título III de la Ley 2/23, art. 21 de la Ley búlgara, y art. 9 de la Ley italiana para el canal externo, gestionado por ANAC.

³⁰ En España la Autoridad Independiente para la Protección de Denunciantes (A.A.I.), en Italia ANAC y en Bulgaria la Comisión de Protección de Datos Personales.

Por ejemplo, el **5º Plan de Acción Nacional (5NAP) para el Gobierno Abierto (2021-2023) de Italia**³¹, se centró en fortalecer la colaboración entre los actores institucionales y de la sociedad civil para apoyar a las personas informantes y crear conciencia.

Los resultados clave incluyeron:

- A. Fomento de la visibilidad y la accesibilidad a los servicios de apoyo de las OSC:** La Autoridad Nacional Anticorrupción (ANAC) lideró un grupo de trabajo en el que participaron la sociedad civil y las administraciones públicas para identificar prácticas para mejorar los estándares de protección de informantes y la calidad de las denuncias. A través de una serie de diálogos conjuntos con ANAC, las aportaciones de las OSC se integraron en el proceso de transposición legislativa de la Directiva, influyendo en la inclusión de una lista pública de OSC que apoyan a las personas denunciantes en el sitio web de ANAC. De este modo, los posibles informantes que acceden al sitio web de ANAC para conocer los procedimientos de denuncia y las salvaguardias relacionadas también se dan cuenta inmediatamente de los servicios de apoyo dedicados a ellos. Esto ha demostrado tener un efecto dominó, ya que otras administraciones públicas italianas han adoptado a su vez la buena práctica de aumentar la visibilidad de los servicios de la sociedad civil proporcionando un enlace directo a su sitio web.
- B. Fortalecimiento de las competencias de los funcionarios públicos a través de una Comunidad de Práctica (CoP):** Bajo el liderazgo de la Escuela Nacional de Administración (SNA), se creó la Comunidad de Práctica de actores institucionales formalmente encargados de la prevención de la corrupción en las administraciones públicas italianas (Responsabile della prevenzione della corruzione e della trasparenza o RPCTs): un espacio de colaboración donde los RPCTs pueden intercambiar conocimientos, compartir mejores prácticas y mejorar sus capacidades para prevenir la corrupción dentro de sus respectivas organizaciones. Con el fin de fortalecer las capacidades de los funcionarios públicos para manejar las denuncias de irregularidades y aumentar su conciencia más amplia sobre la denuncia de irregularidades, la CoP realizó 14 sesiones sobre temas relacionados con la denuncia de irregularidades y superó los objetivos de participación. Se publicó un manual exhaustivo para orientar a los profesionales³², y se han elaborado tres buenas prácticas relativas a la denuncia de irregularidades³³. Los materiales de formación y orientación son vitales para promover la información sobre los sistemas de presentación de denuncias interna y externamente de las administraciones públicas.

Para aumentar la apropiación de los mecanismos de denuncia de irregularidades, todas las entidades obligadas pueden promover la formación de sus directivos y empleados. En la experiencia de las OSC, la **formación dirigida a actores de todos los sectores debería** alejarse de un enfoque centrado en el derecho y **adoptar un enfoque de dilema ético**. A través de esta metodología, que es más experiencial que teórica, los participantes reflexionan sobre casos prototípicos de mala conducta, trabajando tanto individualmente como en grupos para identificar posibles soluciones, incluidas las denuncias de denuncias, ayudándoles a simular una denuncia. Los módulos de formación pueden ser organizados de forma conjunta por las instituciones y otras partes interesadas, como en el ejemplo del proyecto «Open the Whistle (OPWHI)».

Otras iniciativas coherentes con los principios de transparencia y colaboración del OG pueden ser promover **campañas de comunicación conjuntas** entre diversas partes interesadas, siguiendo el ejemplo de "Open the Whistle", o aprovechar los medios de difusión nacionales para proyectos de comunicación con valor social. Las plataformas populares, como las relacionadas con eventos deportivos o culturales, pueden ofrecer oportunidades de comunicación dirigidas a un público muy amplio.

³¹ Ver: <https://www.opengovpartnership.org/members/italy/>

³² Ver: <https://sna.gov.it/wp-content/uploads/2024/09/WHISTLEBLOWING-cultura-integrita.pdf>

³³ El primero hace hincapié en la necesidad de considerar a los denunciantes como una medida humana contra la corrupción; la segunda mejor práctica se centra en el desarrollo de políticas que traten la denuncia como un deber y no como una actividad riesgosa, con el fin de eliminar el estigma social y normalizar el acto de denunciar irregularidades; el tercero hace hincapié en el papel de las Organizaciones de la Sociedad Civil (OSC), proporcionando un enlace directo a su sitio web en la plataforma de denuncia de irregularidades de las AP. <https://sna.gov.it/home/attivita/comunita-di-pratica/comunita-di-pratica-per-rpct/buone-pratiche/whistleblowing-buone-pratiche/>

1.3 TRANSPARENCIA DE LOS SISTEMAS Y CANALES DE INFORMACIÓN: REQUISITOS DE FORMA Y ACCESIBILIDAD

En relación con los requisitos de forma y accesibilidad, cabe destacar que no basta con proporcionar datos genéricos sobre los aspectos anteriormente descritos, sino que esta información debe cumplir una serie de principios y requisitos formales de accesibilidad. Es decir, debe proporcionarse de manera **clara, correcta, completa y actualizada**.

Por ejemplo, la Ley 2/2023 establece explícitamente que se debe facilitar información adecuada de forma clara y fácilmente accesible y que: "En caso de contar con una página web, dicha información deberá constar en la página de inicio, en una sección separada y fácilmente identificable".

Además, el acceso debe ser **universal**, lo que significa que todos los destinatarios potenciales deben tener las mismas oportunidades para acceder a la información. Esto requiere adoptar métodos inclusivos para todas las personas. Según la **Organización Mundial de la Salud (OMS)**, más de mil millones de personas en todo el mundo tienen algún tipo de discapacidad, y de ellas, casi 200 millones experimentan dificultades significativas en su funcionamiento diario³⁴. Los tipos de discapacidad más comunes suelen ser: visuales, auditivas, motoras y cognitivas.

En este sentido, por ejemplo, en **España** hay que tener en cuenta tanto el Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones móviles del sector público, como las Pautas de Accesibilidad al Contenido Web (WCAG) desarrolladas por el World Wide Web Consortium (W3C). Del mismo modo, en Italia³⁵, el Decreto Legislativo n.º 76/2020, por el que se modifica la Ley 4/2004 con la introducción del apartado 1 bis en el artículo 3, amplió la aplicación de las obligaciones de accesibilidad a las entidades privadas, además de a los sitios web del sector público, que ya estaban obligados a ser accesibles.

De acuerdo con estas directrices, es importante evitar ciertas prácticas en los sitios web, como colocar elementos en los que se puede hacer "clic" muy cerca unos de otros y utilizar iconos muy pequeños o enlaces de texto con tamaños de letra excesivamente pequeños. También es recomendable tener en cuenta los contrastes correctos entre las combinaciones de colores de fondo y texto. En este sentido, las WCAG definen en el Criterio 1.4.3, los parámetros que se deben seguir a la hora de establecer el contraste de color³⁶.

Por último, se recomienda que, para facilitar **la comprensión y accesibilidad**, se incluya un apartado de preguntas frecuentes (FAQs) o vídeos explicativos sobre el funcionamiento básico del canal de denuncias. Además, cuando se pongan a disposición de los usuarios archivos multimedia o audiovisuales, estos deben incluir subtítulos, transcripciones de audio y descripciones de video para garantizar el acceso a las personas con discapacidad auditiva.

³⁴ Recuperado de: <https://www.paho.org/es/noticias/5-12-2011-mil-millones-personas-viven-con-discapacidades#:~:text=M%C3%A1s%20de%20mil%20millones%20de,pues%20su%20prevalencia%20est%C3%A1%20aumentando>

³⁵ Para más información, consulte: <https://www.agid.gov.it/ambiti-intervento/accessibilita-usabilita>

³⁶ Por ejemplo, para el nivel AA, se requiere una relación de contraste de 4,5:1 entre el fondo y el texto.

1.4 TRANSPARENCIA DE LOS SISTEMAS Y CANALES DE INFORMACIÓN: INFORMES ANUALES Y ESTADÍSTICAS

La publicación periódica de los datos sobre el rendimiento del sistema en los informes anuales sirve como un ejercicio de **buena gobernanza** y **rendición de cuentas**, y también es una forma de fomentar la confianza.

Como buena práctica, se recomienda proporcionar información estadística **al público y a las partes interesadas**, al menos una vez al año, sobre las siguientes áreas:

- A. Número y tipología de las comunicaciones recibidas.
- B. Número de comunicaciones aceptadas para su tramitación.
- C. Número de comunicaciones desestimadas o archivadas después de realizar la prueba de admisibilidad.
- D. Número de comunicaciones investigadas que terminan en una resolución.
- E. Número de comunicaciones investigadas que han llevado a la adopción de medidas concretas para la mitigación de los daños detectados.
- F. Número de sanciones impuestas o procedimientos disciplinarios iniciados.
- G. Número de veces que la entidad remitió casos a la Fiscalía, a la Fiscalía Europea, a las Autoridades Independientes o a los tribunales.
- H. Número de sesiones de formación o talleres realizados para empleados y directivos en el canal de denuncias.
- I. Número de denuncias confidenciales y número de denuncias anónimas.
- J. Número y tipología de las consultas realizadas.
- K. Número de casos en los que la entidad contrató a una empresa externa para contratar servicios de investigación o expertos en cumplimiento forense.
- L. Número y tipología de las medidas de apoyo³⁷ u otras medidas facilitadas voluntariamente.
- M. En el caso de una organización con presencia internacional: número de comunicaciones recibidas por área geográfica.
- N. Número y tipología de mejoras introducidas en el sistema y canal de información.
- O. Resultados generales sobre el nivel de satisfacción, conocimiento y comprensión del sistema entre las personas destinatarias.

Cabe señalar que los informes o cuentas anuales que elaboren las entidades responsables de la gestión de canales de denuncia **no deben incluir en ningún caso datos de carácter personal**, especialmente aquellos que puedan conducir a la identificación o reidentificación de personas informantes, personas afectadas, testigos u otros terceros involucrados en los procedimientos. Esta restricción aplica incluso en situaciones en las que dichos datos hayan sido previamente divulgados en virtud de una sentencia firme, ya que la finalidad de estos informes es ofrecer información estadística, institucional y de rendición de cuentas, sin comprometer la

³⁷ Descrito en el artículo 37 de la Ley 2/23, art. 13 de la ley búlgara, art.18 del Decreto Legislativo italiano.

confidencialidad, protección de datos y seguridad jurídica de las personas implicadas. Incluir información identificable supondría una vulneración de los principios fundamentales del sistema de protección a los informantes, afectando negativamente la confianza en los mecanismos de integridad institucional. Por tanto, es fundamental que las entidades implementen mecanismos técnicos y organizativos adecuados para anonimizar o disociar los datos, garantizando así el cumplimiento de la normativa sobre protección de datos personales y los estándares internacionales en la materia.

1.5 COMUNICACIÓN INTERNA Y EXTERNA

Los sistemas de denuncia de irregularidades requieren también estrategias de comunicación y concienciación bien diseñadas para garantizar su accesibilidad y generar confianza entre las personas informantes. Sin embargo, persisten varios retos, como la falta de conocimiento sobre los canales de denuncia, la percepción negativa de las personas informantes en algunas culturas, el miedo a las represalias y la ausencia de campañas de concienciación efectivas.

1.5.1 COMUNICACIÓN INTERNA: RETOS Y MEJORES PRÁCTICAS

Falta de claridad e insuficiente formación

Los resultados de las entrevistas a expertos revelaron que muchos empleados desconocen cómo denunciar las irregularidades, y las entidades no brindan información suficiente sobre sus canales internos de denuncia. Para abordar este problema, es recomendable implementar sesiones de capacitación periódicas, campañas de concienciación sobre la denuncia de irregularidades en los programas de incorporación de empleados y reforzar las campañas internas que destaquen la importancia de informar sobre irregularidades. Como **buena práctica**, algunas empresas han implementado códigos QR en diversos materiales con instrucciones claras para facilitar el acceso al canal de denuncias.

Desconfianza y percepción negativa

Según los expertos entrevistados, la denuncia de irregularidades todavía se percibe como un acto de traición en algunos contextos. Las entrevistas indicaron que el miedo es la principal barrera, lo que hace que un cambio en la narrativa sea fundamental. Para superar esto, las estrategias de comunicación deben enfatizar la denuncia de irregularidades como un derecho y una responsabilidad ética, respaldada por testimonios de empleados o líderes que destaquen su importancia e informar claramente sobre las medidas de protección.

Integración con políticas de ética y cumplimiento

Las entrevistas también indicaron que muchas entidades carecen de un compromiso real con el establecimiento de un sistema de información y de cultura de la denuncia de irregularidades. Para fortalecer estos mecanismos, los sistemas de denuncia de irregularidades deben integrarse en las

auditorías internas y en los sistemas de control de riesgos, asegurando su integración en el marco del gobierno corporativo.

1.5.2 COMUNICACIÓN EXTERNA Y PARTICIPACIÓN DE LAS PARTES INTERESADAS

Falta de transparencia y mala comunicación pública

Muchas organizaciones no logran comunicarse de manera efectiva sobre sus sistemas de denuncia de irregularidades. Una medida para cambiar la narrativa podría ser publicar estadísticas e historias de éxito para generar confianza. La proliferación de canales de denuncia mal gestionados ha creado confusión en lugar de fomentar su uso. Para mejorar esta situación, se sugiere por parte de las partes entrevistadas:

- A Informar adecuadamente, por una parte, sobre todos los elementos destacados en la sección 2 de este capítulo de manera clara, correcta, completa y accesible, y por otra, publicar informes anuales con las características mencionadas en el epígrafe anterior; y
- B. Desarrollar campañas estratégicas de sensibilización y acciones clave de sensibilización en colaboración con la sociedad civil.

Papel de la sociedad civil y los medios de comunicación

El papel de la sociedad civil y los medios de comunicación deviene crucial para fortalecer la transparencia y consolidar una cultura de la integridad en el sector público y privado. Según las personas entrevistadas, las organizaciones de la sociedad civil pueden actuar como aliadas estratégicas en la promoción y defensa de los derechos de las personas informantes, especialmente en contextos donde persiste un fuerte estigma social asociado a la denuncia de irregularidades. Este estigma, alimentado por el miedo a represalias o al descrédito personal, sigue siendo una barrera significativa para la participación activa de los ciudadanos en los mecanismos de control democrático. Para revertir esta situación, es imprescindible fomentar canales de diálogo y colaboración entre instituciones públicas, medios de comunicación y organizaciones no gubernamentales, con el objetivo de **dar visibilidad al valor social de la denuncia de irregularidades, proteger a quienes informan de buena fe y ampliar el alcance del ámbito objetivo y subjetivo de los canales de denuncia**. Además, el respaldo público de la sociedad civil y una cobertura mediática responsable pueden contribuir a crear un entorno más seguro y receptivo para quienes deciden alzar la voz frente a la corrupción, el fraude o las malas prácticas.

1.6 RECOMENDACIONES

1. GARANTIZAR UNA TRANSPARENCIA MATERIAL

Asegurar una transparencia completa y significativa³⁸ es fundamental para garantizar una mayor confianza³⁹.

2. MAYOR CLARIDAD

Es crucial asegurar que se brinda **información clara, completa, coherente, actualizada y accesible** sobre los canales y procesos internos de denuncia y que el acceso a los canales se encuentra en una sección de la web fácilmente identificable.

3. CAMBIO DE PERCEPCIÓN

Es clave **cambiar la percepción** de la denuncia de irregularidades como algo vinculado con la deslealtad a las entidades o nociones negativas por una visión de responsabilidad ética y social y un paradigma de que alertar protege a todas las personas.

4. CANALES EXTERNOS Y CENTROS DE APOYO

Brindar toda la información sobre los canales externos para que las potenciales personas informantes puedan decidir qué canal utilizar, así como dar a conocer los centros de apoyo (cívicos e institucionales) ayuda a las personas que se encuentran en dilema ético y no sentirse solas.

5. INCIDENCIA E INCLUSIVIDAD

Generar estrategias inclusivas, con perspectiva de género y protección para las personas informantes en mayor riesgo no es algo opcional sino necesario.

6. FORMACIÓN

Formar a los trabajadores, a los ciudadanos, así como a **los responsables** de la gestión de los sistemas de información es un aspecto clave.

7. CONCLUSIÓN: HACIA UNA CULTURA DE LA TRANSPARENCIA

Transparencia, confianza y eficacia se posicionan como una unidad trimembre estrechamente vinculada para la consecución de los fines de la normativa de protección de informantes. El fortalecimiento de la **transparencia y la comunicación** dentro de las organizaciones constituye un pilar esencial para construir una cultura de denuncia de irregularidades

³⁸ Es muy importante explicar en las webs los pasos para explicar a los denunciantes qué tienen que hacer y cuáles son los procedimientos y sus derechos y obligaciones.

³⁹ Según uno de nuestros entrevistados, también sería importante que las administraciones incluyeran también herramientas, recursos y datos de contacto sobre las organizaciones de la sociedad civil que apoyan a los denunciantes.

que sea **eficaz, accesible y confiable**. Una comunicación clara, proactiva y coherente permite que los miembros de la organización comprendan no solo la existencia de canales de denuncia, sino también su funcionamiento, garantías y objetivos. A su vez, la transparencia en la gestión de estos mecanismos —incluyendo la rendición de cuentas sobre su uso y resultados— contribuye a generar confianza en el sistema, reduciendo el temor a represalias y aumentando la disposición a reportar conductas indebidas. Esta confianza se traduce en una mayor participación y compromiso con los valores éticos, reforzando así una cultura organizativa basada en la **integridad, la legalidad y la responsabilidad compartida**. En definitiva, una política de transparencia acompañada de una comunicación efectiva no solo mejora el control interno, sino que proyecta hacia el exterior una imagen institucional coherente con los principios de buen gobierno.



Investigación y gestión adecuada en los sistemas internos de denuncia



Capítulo 2

INVESTIGACIÓN Y GESTIÓN ADECUADA EN LOS SISTEMAS INTERNOS DE DENUNCIA

Capítulo 2

2.1 CLAVES PARA UNA INVESTIGACIÓN ADECUADA

Tal y como ya se señaló en el capítulo anterior, el marco jurídico definido por la Directiva 2019/1937 depende de una condición crucial para su eficacia: *la confianza en el sistema*. Cuando una denuncia interna cubierta por el ámbito de aplicación objetivo y subjetivo de la Directiva y las leyes nacionales se reciba en los canales de información, podrá iniciarse una investigación interna que deberá cumplir con todas las garantías legales y procesales y ser objeto de un seguimiento diligente. Los canales de denuncia internos y externos deben ofrecer salvaguardias adecuadas contra posibles *represalias*, lo que constituye una piedra angular para alentar a las personas informantes a denunciar y romper el silencio.

El artículo 7, apartados 1 y 2, de la Directiva establece el principio de que las personas informantes son libres de elegir si informan primero internamente o directamente a través de canales externos. La denuncia externa está especialmente prevista en situaciones en las que la violación no puede abordarse eficazmente internamente, o cuando la persona informante considera que no hay riesgo de represalias (véase el párrafo 2 del artículo 7). Varios Estados miembros (que no se identifican en el informe) imponen incorrectamente la obligación de informar primero internamente o permiten la presentación de denuncias externas directas solo en circunstancias específicas. Además, algunos Estados miembros no han proporcionado explícitamente protección a las personas que informan a las instituciones de la UE. En este contexto, la presentación de denuncias internas es el medio más adecuado de recopilación de información para una resolución temprana de las amenazas al interés público. Por este motivo, **se da preferencia a los canales internos de denuncia**, aunque la presentación de denuncias internas no es un requisito previo obligatorio para la presentación de denuncias externas.

La segunda reunión del grupo de expertos de la Comisión Europea sobre la Directiva⁴¹ señala que cuando las personas informantes informan directamente a través de canales externos, las organizaciones no pueden remediar rápidamente la situación o la irregularidad. En consecuencia, las organizaciones deben establecer canales internos claros, de fácil acceso y eficaces, y fomentar una **cultura corporativa** que fomente activamente la denuncia interna de infracciones. Las investigaciones internas derivadas de las comunicaciones o la información recibida a través de canales internos, ya

⁴¹ El grupo de expertos de la Comisión Europea es un grupo consultivo formado por expertos que representan a los Estados miembros de la Unión Europea con responsabilidades en la transposición de la Directiva 2019/1937/UE. Su misión fundamental es elaborar recomendaciones a los Estados miembros para la transposición de la Directiva 2019/1937/UE.

sea dentro de una organización pública o privada, se llevan a cabo **en aras del interés público**.

Los procedimientos internos de presentación de denuncias y su seguimiento deben cumplir determinados requisitos fundamentales para alcanzar el objetivo previsto y cumplir las disposiciones de la Directiva y de la legislación nacional. Estos requisitos son esencialmente los siguientes:

- A. Los canales internos deben permitir a las personas incluidas en el ámbito de aplicación personal de la Directiva denunciar las infracciones cubiertas por su ámbito de aplicación material y las leyes nacionales de transposición.
- B. Los canales deben diseñarse, establecerse y gestionarse de forma segura para garantizar la confidencialidad de la identidad de la persona informante y de cualquier tercero mencionado en el informe, al tiempo que se protegen los datos personales y del acceso no autorizado.
- C. Se debe emitir un acuse de recibo al demandante dentro de los siete días posteriores a la recepción del informe.
- D. La comunicación con la persona informante podrá mantenerse durante la tramitación de la denuncia, pudiendo solicitarse información adicional en caso de ser necesario.
- E. Los canales deberán permitir un seguimiento diligente y un tratamiento eficaz de las comunicaciones presentadas, incluidas las anónimas, cuando corresponda.
- F. Deberá facilitarse información clara y accesible sobre los canales externos gestionados por las autoridades nacionales competentes y, en su caso, por las instituciones u organismos de la UE.

PERSPECTIVA DE GÉNERO

La aplicación de canales sensibles a las cuestiones de género y políticas específicas mejoraría la eficacia de los procesos de apoyo, en particular para las mujeres y otros grupos vulnerables.

Entre **las recomendaciones específicas para garantizar que los canales denuncias tengan en cuenta las cuestiones de género se incluyen las siguientes:**

- A. **Diseño y representación inclusivos.** Garantizar la participación de las mujeres y las diversas identidades de género en el diseño de los mecanismos y políticas de denuncia.
- B. **Protocolos y coordinación con perspectiva de género.** Establecer protocolos de género para cada canal interno de denuncia. Coordinar los esfuerzos entre los mecanismos de código de conducta, lucha contra la corrupción y denuncia de la violencia de género.
- C. **Sistemas de denuncia e investigación con perspectiva de género y servicios de apoyo integrales.** Directrices claras para los casos basados en el género, con personal capacitado para manejar las denuncias con sensibilidad. Informar a las personas denunciantes sobre los servicios de apoyo externo, como la asistencia jurídica, el apoyo psicológico y las organizaciones de defensa de los supervivientes.
- D. **Preguntas frecuentes y canales de soporte con perspectiva de género.** Desarrollar un canal específico para consultas relacionadas con conductas indebidas basadas en el género. Proporcionar una sección de preguntas frecuentes (FAQ) o pautas claras para informar sobre cuestiones relacionadas con el género.
- E. **Sensibilización y formación.** Llevar a cabo capacitaciones de concienciación y sensibilización basadas en el género dentro de las organizaciones que disponen de canales de denuncia. Abordar los estereotipos y sesgos de género para garantizar un sistema de denuncia de irregularidades inclusivo y eficaz.

2.2 DESAFÍOS DE LAS INVESTIGACIONES INTERNAS

Las investigaciones internas **tienen como objetivo verificar la veracidad o verosimilitud de los hechos denunciados** e identificar a las personas responsables de la violación o irregularidad en cuestión. Es especialmente importante, tanto para la validez de las propias investigaciones internas como para garantizar el cumplimiento de la Directiva y de las legislaciones nacionales, que todos los métodos utilizados para reunir pruebas respeten los derechos fundamentales en todos los casos.

¿Cuáles son los desafíos que pueden surgir durante la investigación interna?

- A. Mantener la **confidencialidad** de los datos personales puede ser complejo y requiere la implementación de medidas técnicas, **organizativas y de seguridad específicas** (como el acceso restringido y jerárquico, la doble autenticación, la anonimización interna, etc.) diseñadas explícitamente para este fin. Durante **las investigaciones internas**, la identidad de la persona informante puede descubrirse o deducirse inadvertidamente, ya que ciertas características (por ejemplo, género, puesto de trabajo, proyecto asociado, etc.) pueden revelar indirectamente su identidad. Además, solicitar información a otros departamentos o realizar entrevistas personales puede ampliar inevitablemente el **círculo de personas** al tanto de la investigación y, potencialmente, de la identidad de la persona informante, por lo que es importante contar con políticas y protocolos de seguridad y de investigación sólidos y personal formado en la materia.
- B. Garantizar la **confidencialidad de la identidad de las personas informantes** cuando los canales internos de denuncia se externalizan a un tercero (subcontratista). Dicha externalización debe cumplir lo dispuesto en **el considerando 54 de la Directiva de la UE**, que especifica que **entre los terceros** pueden figurar proveedores externos de plataformas de denuncia, asesores externos, auditores, representantes sindicales o representantes de los trabajadores. La subcontratación aumenta inherentemente el número de personas con acceso a información confidencial. Por lo tanto, **las garantías explícitas de independencia** y confidencialidad deben estar claramente descritas en el acuerdo contractual entre la organización y el tercero externo. De conformidad con el artículo 8, apartado 5, de la Directiva, en caso de incumplimiento, tanto el tercero como la persona jurídica comparten la responsabilidad. **Las personas expertas entrevistadas consideran que la responsabilidad solidaria** es la forma más eficaz de proteger los derechos de las y los denunciantes, permitiendo a la persona denunciante iniciar acciones legales contra la entidad, el tercero externo o ambos.
- C. **El tratamiento de la identidad de una persona informante** constituye un "tratamiento de datos personales", en el sentido del Reglamento General de Protección de Datos (RGPD). En consecuencia, **las sanciones** por revelar la identidad de la persona informante deben ser más severas que **las sanciones** generalmente previstas por las legislaciones nacionales para otras violaciones de la confidencialidad de los datos personales. Esta mayor severidad es necesaria porque revelar la identidad de la persona informante **puede exponerla** a represalias y debilitar la confianza en el propio sistema de denuncias.

- D. Las sanciones por violaciones de la confidencialidad se han transpuesto incorrectamente en ciertos casos, por ejemplo, debido a la **falta de referencias cruzadas adecuadas** a la legislación aplicable. Esta situación es especialmente preocupante, en primer lugar, por la falta de armonización de los **estándares europeos de protección y**, en segundo lugar, porque socava uno de los pilares de la regulación europea de las personas denunciantes.
- E. Durante las investigaciones internas, también entran en juego los intereses privados de las organizaciones. En consecuencia, en determinados contextos, las investigaciones internas sobre incumplimientos e irregularidades se consideran mecanismos de **colaboración público-privada**. Sin embargo, las entrevistas realizadas en **Italia** han puesto de manifiesto un desafío específico: pueden surgir conflictos de interés cuando el contenido del informe de la persona informante entra en conflicto con los intereses de la organización.

PERSPECTIVA DE GOBIERNO ABIERTO

La investigación y la gestión eficaces de los sistemas internos de presentación de denuncias requieren **transparencia y directrices bien definidas** para garantizar la coherencia y la equidad en los diferentes sectores, incluidos el sector público, el sector privado y las organizaciones sin fines de lucro. Dichas directrices pueden desarrollarse a través de un enfoque de diseño conjunto, en el que participen las autoridades públicas responsables de la denuncia de irregularidades y las partes interesadas. Este proceso de colaboración puede tener lugar a través de **diálogos o consultas públicas**, como lo demuestra la Autoridad Nacional Anticorrupción (ANAC) italiana.

En 2024, ANAC lanzó una consulta pública en línea⁴² para recopilar comentarios sobre su borrador de directrices para la denuncia de irregularidades. El objetivo era promover una aplicación uniforme y eficaz de la legislación en materia de denuncia de irregularidades, al tiempo que se reducían las incertidumbres interpretativas para las entidades que gestionan denuncias internas tanto en organizaciones públicas como privadas. El modelo de ANAC proporciona un marco útil que otros países podrían replicar para mejorar la participación de las partes interesadas en el desarrollo de directrices para la denuncia de irregularidades:

- A. Un período de consulta en línea abierto de al menos un mes para permitir tiempo suficiente para la retroalimentación.
- B. Una plataforma fácil de usar para enviar contribuciones (por ejemplo, cuestionarios en línea).
- C. Amplia difusión de la iniciativa en múltiples foros pertinentes para garantizar la visibilidad y fomentar la participación.
- D. Invitaciones específicas a las partes interesadas clave que participan activamente en los procesos de denuncia de irregularidades.

Los profesionales recomiendan designar un **punto de contacto específico dentro de la autoridad pública responsable de la denuncia de irregularidades**. Esta persona actuaría como un recurso para los gerentes de los canales de denuncias internas, proporcionando orientación y resolviendo desafíos en la gestión e investigación de denuncias. Además, las preocupaciones relacionadas con la investigación adecuada de las denuncias podrían abordarse mediante reuniones entre pares entre los responsables del canal de denuncias internas y la autoridad pública. Para fomentar la colaboración y la mejora continua, la creación de un grupo de **trabajo o Comunidad de Práctica** sobre denuncia de irregularidades podría incorporarse a la Alianza para el gobierno abierto, ya sea como parte

⁴² Ver: <https://www.anticorruzione.it/en/-/news.07.11.24.lg.whistleblowing>

de los Planes de Acción Nacionales regulares o como un compromiso del Open Gov Challenge.

Otro aspecto clave para facilitar una investigación adecuada es garantizar la alta calidad de los informes de denuncia. Una forma eficaz de diseñar un sistema de informes internos sólido, que sea lo más preciso posible y esté alineado con los riesgos reales a los que se enfrenta la organización (ya sea pública o privada), es realizar una **evaluación de riesgos participativa de las posibles conductas indebidas que podrían surgir a través de la denuncia de irregularidades**.

Lo ideal es que este proceso involucre a múltiples departamentos, áreas y sectores dentro de la organización. Sin embargo, particularmente en el caso de las instituciones públicas, también se puede llevar a cabo utilizando los principios del gobierno abierto involucrando a la sociedad civil en la configuración del proceso. Las aportaciones externas pueden proporcionar una perspectiva más amplia y una comprensión más profunda de los factores ambientales y contextuales, lo que ayuda a la organización a identificar riesgos que, de otro modo, podrían pasarse por alto o subestimarse. El resultado de este proceso es un sistema de informes que incluye escenarios de casos bien definidos, adaptados a una comprensión más profunda de los riesgos de la organización. Esto no solo ayuda a las personas informantes a redactar informes más claros y precisos, sino que también garantiza una investigación más eficaz y exhaustiva.

2.3 MARCO GENERAL DE LOS PROCEDIMIENTOS DE INVESTIGACIÓN

El artículo 9, apartado 1, de la Directiva establece que el procedimiento interno de denuncia debe incluir un **seguimiento diligente** por parte de la persona o el servicio designado a tal efecto (véase el [capítulo 1](#) sobre la transparencia en el procedimiento de denuncia de irregularidades).

A este respecto, el artículo 5.12 de la Directiva define el "seguimiento" como:

"Cualquier medida adoptada por el destinatario de un informe o cualquier autoridad competente para evaluar la exactitud de las alegaciones formuladas en el informe y, cuando proceda, para hacer frente a la violación denunciada, incluso mediante acciones tales como una investigación interna, una investigación, un enjuiciamiento, una acción para la recuperación de fondos o el cierre del procedimiento".

Por lo tanto, la Directiva incluye dos acciones en el concepto de **seguimiento diligente del informe**: la evaluación de la exactitud de los problemas notificados y la resolución de la infracción denunciada.

Según el **Informe sobre la aplicación de la Directiva**, en la mayoría de los Estados miembros no se han transpuesto correctamente varios componentes de esta disposición (artículo 9), como la obligación de realizar un seguimiento diligente de las denuncias, los plazos para emitir un acuse de recibo o la organización de reuniones presenciales. La legislación nacional de transposición establece generalmente un **cierto contenido mínimo y/o principios** para los procedimientos internos de notificación, aunque normalmente no los regula en detalle. Por lo tanto, las entidades obligadas conservan cierto margen de discrecionalidad para autorregularse y organizar investigaciones internas, siempre que respeten los principios y requisitos mínimos definidos por la legislación nacional. Esto permite que los procedimientos se adapten mejor a las características de cada organización.

En España, **el artículo 9.2 de la Ley 2/2023** establece que el procedimiento de denuncia interna debe cumplir con una serie de principios y requisitos mínimos, entre los que se encuentran la identificación clara de los canales de denuncia internos y externos, la emisión de un acuse de recibo a la persona informante en un plazo de siete días y el establecimiento de un plazo máximo de tres meses para responder a las investigaciones, prorrogable en casos complejos. Además, se debe permitir la comunicación continua con la parte denunciante, garantizando su derecho a ser informado sobre el progreso de su denuncia. También se debe garantizar la confidencialidad, la presunción de inocencia, la protección de datos personales y el respeto al honor de los involucrados. Si los hechos denunciados pueden constituir una infracción penal, la información debe transmitirse a la Fiscalía o, si los intereses financieros de la UE están implicados, a la Fiscalía Europea.

Un requisito similar existe en **Italia**, donde el **artículo 4 del Decreto Legislativo 24/2023** establece que tanto las entidades del sector público como las del sector privado deben establecer canales que garanticen la confidencialidad de la identidad de la persona denunciante, de las personas implicadas o mencionadas en la denuncia, así como del contenido de la denuncia y de la documentación que la acompaña, incluso mediante herramientas de cifrado.

Los procedimientos y protocolos aprobados por los obligados deben definir claramente los principios generales que rigen los canales internos de denuncia y la protección de la persona denunciante dentro de la organización. Estos procedimientos deben ser aprobados formalmente por el órgano administrativo o de gobierno de la entidad. Además, deben ser publicados y comunicados de manera efectiva a todos los usuarios potenciales del canal. La difusión adecuada es esencial, ya que ayuda a prevenir el uso indebido del canal y reduce los envíos que no se pueden procesar adecuadamente.

2.3.1 PROCEDIMIENTO DE INVESTIGACIÓN: DIRECTRICES, PRINCIPIOS Y GARANTÍAS

Para **garantizar la seguridad jurídica** en las investigaciones internas y proteger a **los propios investigadores**, es **muy aconsejable que** los procedimientos internos de gestión de denuncias se detallen de forma exhaustiva. Más allá del contenido mínimo y los principios esbozados por las leyes nacionales de transposición, los procedimientos internos **deben describir explícitamente** cada fase del proceso de gestión de la presentación de denuncias, **especificando las acciones** que deben realizarse en cada fase. Estos procedimientos también deben regular los métodos de verificación y esbozar las medidas adecuadas para preservar y salvaguardar la documentación y las pruebas reunidas durante las investigaciones.

Las fases del procedimiento de información interna que podrían incluirse en el procedimiento son las siguientes:

- A. Fase de recepción de denuncias.
- B. Fase de admisión o inadmisión.

- C. Fase de investigación.
- D. Fase de finalización o terminación de la investigación.

2.4 DERECHOS DE LAS PERSONAS INFORMANTES

La persona denunciante tiene el **derecho fundamental** a presentar una denuncia confidencial y a no revelar su identidad, cuando lo permita la legislación nacional.

Denuncias anónimas

La Directiva y cualquier legislación de transposición establecen la obligación de mantener la confidencialidad de la identidad de la persona informante y del contenido de la denuncia. Por lo que respecta a las denuncias anónimas, la Directiva permite diferentes enfoques nacionales, ya que no todos los Estados miembros aceptan la denuncia anónima. No obstante, cuando esté permitido, **deberá garantizarse la comunicación con los y las denunciantes anónimos.**

En **el Informe sobre la aplicación de la Directiva** publicado por la Comisión, se hace hincapié en que, si los Estados miembros exigen a las entidades que acepten denuncias anónimas, **dichas denuncias deben tramitarse con los mismos derechos procesales que las denuncias no anónimas.** Esto incluye tanto los derechos de la persona informante como las obligaciones de las entidades y autoridades de realizar un seguimiento diligente.

Dado que una investigación interna puede dar lugar a **procedimientos disciplinarios, sancionatorios o penales**, las pruebas deben obtenerse de conformidad con las leyes aplicables, las normas de procedimiento y los derechos de todas las partes implicadas. Estos incluyen **los derechos fundamentales, los derechos laborales, los derechos establecidos en la Directiva y la legislación nacional, así como los procedimientos y protocolos internos aprobados por la organización.**

Una buena práctica **ampliamente recomendada** es proteger los derechos de los demandantes mediante **la responsabilidad conjunta**, lo que les permite emprender acciones legales **contra la entidad, contra el tercero externo que administra el sistema de presentación de denuncias o contra ambos.**

- A. Presentar una denuncia verbalmente o por escrito.
- B. Elegir si se denuncia a través del canal interno, a menos que tengan motivos válidos para informar externamente.
- C. A recibir asesoría legal confidencial y gratuita en el momento de la denuncia.

Este consejo debería aclarar:

- A. Si la información denunciada entra en el ámbito de aplicación de las normas de protección de la persona informante.

- B. El canal de denuncia más adecuado a utilizar.
- C. Procedimientos alternativos en caso de que la información no se encuadre dentro de la normativa aplicable en materia de denuncia de irregularidades.
- D. Medidas de protección y apoyo disponibles.
- E. Recibir un acuse de recibo de su informe.
- F. Acceder a medidas de protección y apoyo, incluida la asistencia financiera y el apoyo psicológico en determinados casos, siempre que la persona denunciante cumpla las condiciones de protección. Esto incluye casos en los que denunciaron de forma anónima, fueron identificados posteriormente y sufrieron represalias.
- G. A ser informado sobre el estado de su denuncia y a recibir actualizaciones sobre el resultado de la investigación.
- H. Mantener la confidencialidad y proteger su identidad durante todo el proceso.
- I. A que sus datos personales sean tratados de conformidad con los derechos que les confiere la legislación europea y la legislación nacional en la materia.

Los Estados miembros, en sus leyes de transposición, pueden **introducir disposiciones** más favorables a los derechos de la persona informante que las establecidas en la Directiva. Es importante tener en cuenta que, para tener derecho a la protección, las personas informantes no solo deben denunciar a través de los canales previstos en la Directiva, sino también tener **motivos razonables para creer que, sobre la base de la información de que disponen en el momento de la denuncia, los hechos que revelan son ciertos**. La protección **no se extiende a las denuncias abusivas, maliciosas o falsas**.

La **persona** afectada debe tener los siguientes derechos fundamentales:

- A. A que se preserve su identidad.
- B. A ser informado y a ser oído, en la forma y en el plazo que se considere apropiados para garantizar la eficacia de la investigación.
- C. Acceder al contenido del expediente de las actuaciones investigativas y formular alegatos.
- D. A la presunción de inocencia y al derecho al honor.
- E. Recibir información sobre las medidas adoptadas que les afecten como resultado de la investigación.
- F. A que sus datos personales sean tratados de conformidad con los derechos que les confiere la legislación europea y la legislación nacional en la materia.

De conformidad con **el considerando 76 de la Directiva**, los Estados miembros deben velar por que las autoridades competentes dispongan **de procedimientos adecuados** para tramitar las denuncias y proteger los datos personales de las personas mencionadas en ellas. **Estos procedimientos deben garantizar** la protección de la identidad de cada denunciante y de cada persona afectada, pero también de los terceros mencionados en la denuncia, como testigos o compañeros de trabajo, en todas las fases del procedimiento.

2.4.1 DERECHOS RELACIONADOS CON EL TRATAMIENTO DE DATOS PERSONALES

En cuanto a los derechos vinculados al **tratamiento de datos personales**, cuando los datos se obtengan del interesado, se deberá facilitar la información indicada en el art. 13 del Reglamento (UE) 2016/679.

Las personas denunciantes, los acusados, así como los **terceros mencionados** en las denuncias y en las investigaciones podrán ejercer los derechos reconocidos por los artículos 15 a 22 del Reglamento (UE) 2016/679 (derecho de acceso del interesado, derecho de rectificación, derecho de supresión, derecho a la limitación del tratamiento, obligación de notificación relativa a la rectificación o supresión de datos personales o limitación del tratamiento, derecho a la portabilidad de los datos, derecho de oposición, derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles).

Sin embargo, en algunos casos, las leyes nacionales de transposición **han restringido el ejercicio de determinados derechos**. Por ejemplo, el derecho a oponerse al tratamiento de datos personales por parte de las autoridades competentes se ha limitado en algunas jurisdicciones.

2.5 ESTRUCTURA DE LAS DENUNCIAS INTERNAS Y RESPONSABILIDADES

La decisión **de designar a una persona responsable** del canal interno de denuncias y, en su caso, de personal adicional para gestionar los procedimientos de seguimiento de las denuncias (tal y como se ha establecido en algunos países, como **España**) debe hacerse de forma transparente. Esto significa que los usuarios potenciales del canal **deben ser informados** de la identidad de estas personas. Las personas responsables de gestionar el canal interno **deben poseer los conocimientos técnicos** necesarios, así como las habilidades y competencias necesarias para llevar a cabo investigaciones internas de forma eficaz. Sin embargo, **este requisito de transparencia también presenta retos**, particularmente en el establecimiento de plataformas de comunicación efectivas para personas ajenas a la organización (por ejemplo, contratistas, ex pasantes).

Desde un punto de vista práctico, **especialmente en las grandes organizaciones**, puede ser prácticamente imposible que una sola persona o departamento **maneje todas las denuncias internas enviadas** a través del canal. Además, el artículo 16 de la Directiva exige a los Estados miembros que **garanticen que la identidad** del denunciante no se revele sin su consentimiento explícito, excepto a un miembro del personal autorizado responsable de la tramitación o el seguimiento de las denuncias, tal como se define en el artículo 5, apartado 12, de la Directiva. Esta disposición implica que **un equipo de personas**, con la formación técnica necesaria y sujetas a estrictas obligaciones de confidencialidad, **puede participar en el seguimiento de las denuncias**, analizar los casos desde diferentes perspectivas o realizar diferentes funciones de investigación.

Por lo tanto, **se recomienda:**

- A. **Hacer referencia explícita** a la existencia del canal de denuncia, en cumplimiento de las obligaciones de transparencia establecidas en la

Directiva de la UE en cláusulas contractuales o documentos complementarios

- B. **Designar anticipadamente** a una persona suplente que pueda **sustituir temporal o definitivamente** al responsable que gestiona el canal interno de denuncias en casos de vacante, ausencia o enfermedad. Este **mecanismo de sustitución** también es imprescindible en situaciones en las que el **gestor de canal principal** debe recusarse por conflicto de interés u otros motivos legalmente establecidos.
- C. **Informar plenamente a todas las personas afectadas por un informe del procedimiento de investigación y de la identidad de las personas responsables de llevar a cabo la investigación interna.**

Además, es esencial que las personas afectadas puedan confiar en que quienes gestionan la denuncia actuarán con **objetividad e imparcialidad**. Esta confianza refuerza la legitimidad del sistema y promueve un entorno justo, donde los derechos de todas las partes involucradas son protegidos.

Al garantizar que las denuncias sean procesados e investigados por profesionales neutrales y competentes, las organizaciones aumentarán la confianza y la eficacia en el sistema de denuncias internas. Esto, a su vez, reforzará la confianza entre todos los usuarios potenciales de que el canal de denuncias funciona de forma adecuada y fiable, y de que las denuncias se toman en serio y se gestionan con diligencia. Contar con una disposición de este tipo es crucial para garantizar la objetividad e imparcialidad en las investigaciones internas.

2.5.1 ESTRUCTURA ORGANIZATIVA DE LOS SISTEMAS INTERNOS DE INFORMACIÓN

El órgano de administración o gobierno de una entidad podrá designar a la/s **persona/s responsable/s de la gestión del canal interno de denuncias** y de la gestión de la recepción y seguimiento de las denuncias, tal y como ocurre en la **legislación española e italiana**. Para que el sistema sea eficaz y creíble, todas las comunicaciones deben gestionarse de forma eficiente y diligente dentro de la propia organización. Esta responsabilidad podría recaer en el responsable del canal interno de denuncias. Por lo tanto, es fundamental que estas personas, por su posición dentro de la organización, sean capaces de desempeñar sus funciones de **forma independiente y autónoma**, sin estar sujetas a ninguna influencia externa, y con acceso a todos los recursos personales y materiales necesarios para cumplir su función. Como se mencionó anteriormente, las circunstancias específicas de cada organización pueden justificar la asignación de esta responsabilidad a un equipo en lugar de a un solo individuo. Además de beneficiarse de la toma de decisiones colectiva, un equipo de este tipo también podría aportar una perspectiva multidisciplinaria a las investigaciones.

La selección de los profesionales adecuados puede variar en función del tipo y estructura de la entidad. Sin embargo, los responsables de gestionar el canal de denuncias internas deben estar comprometidos con el cumplimiento normativo, la integridad y los principios y valores éticos de la organización. Ya que estas personas deben desempeñar sus **funciones de manera independiente y autónoma, y en todo caso evitando conflictos de interés**. En última instancia, la credibilidad del sistema de denuncias

internas depende de **la confianza que los empleados depositen en los responsables de manejar las denuncias**. Si los empleados perciben que las denuncias se gestionan de forma objetiva y eficaz, es más probable que utilicen el canal interno.

En las entidades más pequeñas, esta podría ser una doble función llevada a cabo por un ejecutivo de la empresa que está bien situado para **comunicarse directamente** con la gerencia de la entidad, por ejemplo, un especialista de cumplimiento o recursos humanos, un especialista de integridad institucional, un especialista legal o de privacidad, un especialista financiero, un especialista de auditoría o un miembro de la junta directiva.

Con carácter general, la persona responsable del canal interno puede incurrir en responsabilidades derivadas de la gestión y correcto funcionamiento del sistema interno. Dichas responsabilidades pueden estar relacionadas con el tratamiento y seguimiento diligente de las denuncias, con las **garantías de protección** del informante dentro de la propia organización, así como con su comportamiento cuando tiene que interactuar con las autoridades competentes. Además, en ciertos casos, la persona responsable puede incurrir en **responsabilidad penal** si la conducta está tipificada en la legislación penal aplicable (por ejemplo, revelación de secretos, delitos cometidos por funcionarios públicos).

En todo caso, habrá que tener en cuenta las obligaciones establecidas por la legislación nacional de transposición de los Estados miembros a efectos de determinar las responsabilidades específicas de los responsables y gestores del canal interno en cada caso.

2.5.2 CONFLICTOS DE INTERÉS EN LOS SISTEMAS INTERNOS DE INFORMACIÓN

Los conflictos de intereses surgen en situaciones en las que la imparcialidad y la objetividad de las personas responsables de emitir juicios profesionales se ven comprometidas por un interés personal o externo. Como cualquier riesgo, los conflictos de interés pueden y deben gestionarse de forma proactiva. Para garantizar la equidad y la credibilidad, los procedimientos internos de gestión de denuncias deben incluir explícitamente medidas para identificar, gestionar y abordar los conflictos de interés que puedan afectar a los responsables de la gestión e investigación de las denuncias. Esto garantiza que las personas que llevan a cabo investigaciones internas permanezcan imparciales y objetivas.

No es aconsejable adoptar un **enfoque reactivo de los conflictos de interés**, es decir, esperar a que surja un conflicto antes de determinar cómo gestionarlo. En su lugar, las organizaciones **deben anticiparse y establecer** procedimientos claros para abordar tales situaciones. De lo contrario, **se puede socavar** la confianza en el canal interno de denuncias, ya que podrían surgir preocupaciones sobre sesgos o falta de imparcialidad, lo que llevaría a una pérdida de credibilidad en la gestión de las denuncias.

Una **buena práctica reconocida** es exigir a los investigadores que completen una "Declaración de No Conflicto de Interés" antes de iniciar un procedimiento de denuncia interna. Esto ayuda a garantizar que el personal

asignado no tenga vínculos personales o profesionales que puedan afectar su neutralidad.

Las investigaciones tienen un **límite de tiempo**. Deberán durar el tiempo necesario, que no podrá exceder del plazo de tres meses, salvo en los casos de especial complejidad, en los que el procedimiento podrá prorrogarse por tres meses adicionales. La prórroga de tres meses adicionales deberá adoptarse con anterioridad a la conclusión de este primer período, exponiendo las causas que han impedido la conclusión de las investigaciones y las diligencias pendientes, justificando la razón de la adopción de esta prórroga.

2.5.3 CONSIDERACIONES SOBRE LA PROTECCIÓN DE DATOS

El artículo 17 de la Directiva establece que cualquier **tratamiento de datos personales** que se lleve a cabo en aplicación de la misma, deberá cumplir con el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680. Además, **cualquier intercambio o transmisión de información** por parte de las instituciones, órganos, oficinas o agencias de la UE debe llevarse a cabo de conformidad con el Reglamento (UE) 2018/1725, que rige la protección de datos dentro de las instituciones de la UE.

Este artículo también incorpora el principio de minimización de datos, que tiene como objetivo evitar la recopilación de datos innecesarios para la investigación de un informe. Si se recopilan accidentalmente datos irrelevantes, deben eliminarse de inmediato.

Sin embargo, también es fundamental tener en cuenta la legislación nacional en aspectos específicos como el acceso a los datos personales contenidos en el canal interno, el registro de denuncias y los expedientes de investigación, así como los plazos de conservación de los datos establecidos por la legislación nacional.

De conformidad con el considerando 83 de la Directiva, debe prestarse especial atención a los principios fundamentales del tratamiento de datos personales establecidos en el artículo 5 del Reglamento (UE) 2016/679, el artículo 4 de la Directiva (UE) 2016/680 y el artículo 4 del Reglamento (UE) 2018/1725, así como al principio de protección de datos desde el diseño y por defecto establecido en el artículo 25 del Reglamento (UE) 2016/679, el artículo 20 de la Directiva (UE) 2016/680 y los artículos 27 y 85 del Reglamento (UE) 2018/1725.

Es importante recordar el contenido del artículo 5 del Reglamento (UE) 2016/679⁴³ que establece que los **principios rectores para garantizar** la legitimidad del tratamiento de datos personales son el principio de responsabilidad proactiva, el principio de legalidad, lealtad y transparencia, el principio de limitación de la finalidad, el principio de minimización de datos, el principio de exactitud, el principio de limitación del plazo de conservación y el principio de integridad y confidencialidad. (Para leer detalles exhaustivos, véase el **Capítulo 3**.)

2.6 PROCESO DE INVESTIGACIÓN DENTRO DEL SISTEMA INTERNO DE DENUNCIAS

Es recomendable establecer un sistema de identificación de denuncias, junto con un registro de la información recibida y de las investigaciones internas realizadas. Se debe prestar especial atención a la limitación de los períodos de retención de datos personales, **consulte el Capítulo 3** para explorar el tema en profundidad. Durante la fase de recepción de la denuncia, la persona denunciante debe recibir un **acuse de recibo en un plazo de siete días**. Esta confirmación es fundamental, ya que sirve como prueba de que la parte denunciante ha presentado una denuncia a través del **canal interno de denuncias**. También puede ser necesario cuando se soliciten medidas de protección y/o apoyo a la autoridad competente.

Una vez que se recibe una denuncia, la siguiente fase de un protocolo de investigación interna podría ser determinar la **admisibilidad de la misma**. El responsable del canal interno debe valorar la denuncia y decidirse, con motivación, por una de las siguientes opciones:

- A. Inadmisibilidad de la denuncia.
- B. Admisión de la denuncia para su tramitación.
- C. Remisión de la denuncia al Ministerio Fiscal, a la Fiscalía Europea o a cualquier otra autoridad, entidad u organismo competente.

⁴³ 1. Artículo 5. Los datos personales serán:

- a. tratados de manera lícita, leal y transparente en relación con el interesado («licitud, equidad y transparencia»);
- b. recopilados para fines determinados, explícitos y legítimos y no tratados posteriormente de manera incompatible con dichos fines; de conformidad con el , apartado 1, no se considerará incompatible con los fines iniciales el tratamiento ulterior con fines de archivo en interés público, de investigación científica o histórica o con fines estadísticos («limitación de la finalidad»);
- c. adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se tratan («minimización de datos»);
- d. exactos y, en su caso, actualizados; deben adoptarse todas las medidas razonables para garantizar que los datos personales que sean inexactos, teniendo en cuenta los fines para los que se tratan, se eliminen o rectifiquen sin demora («exactitud»);
- e. conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que se tratan los datos personales; los datos personales podrán conservarse durante períodos más largos, en la medida en que los datos personales se traten únicamente con fines de archivo de interés público, de investigación científica o histórica o estadísticos, de conformidad con el 1) sin perjuicio de la aplicación de las medidas técnicas y organizativas adecuadas exigidas por el presente Reglamento para salvaguardar los derechos y libertades del interesado (en lo sucesivo, «limitación del almacenamiento»);
- f. tratados de manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, destrucción o daño accidentales, utilizando medidas técnicas u organizativas adecuadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del apartado 1 (en lo sucesivo, «responsabilidad») y podrá demostrar su cumplimiento.

Ejemplos de criterios de inadmisibilidad:

Una denuncia podrá considerarse inadmisible en las siguientes circunstancias:

- A. Acusaciones ininteligibles e inverosímiles, incluidas denuncias falsas prima facie sin base objetiva.
- B. Denuncias que carezcan de una descripción mínima de los hechos, como la hora, el lugar o la naturaleza de la supuesta infracción o irregularidad.
- C. Denuncias basadas únicamente en rumores, especulaciones, rumores o suposiciones.
- D. Denuncias sobre hechos idénticos ya investigados y resueltos por la organización, a menos que se aporten nuevas pruebas o información significativa.

Por lo que se refiere a la primera causa de inadmisibilidad —denuncias prima facie falsas—, el considerando 101 prevé el mantenimiento de la protección cuando los hechos comunicados sean inexactos o engañosos con arreglo a las normas del Derecho nacional general. Sin embargo, el artículo 23 de la Directiva exige a los Estados miembros que impongan sanciones a las denuncias falsas o malintencionadas a sabiendas, con el fin de evitar nuevas denuncias falsas o malintencionadas y preservar la credibilidad del sistema. Estas sanciones deben ser proporcionadas, garantizando que no tengan un efecto disuasorio sobre las partes denunciantes legítimas. Cuando se trata de denuncias falsas, las entidades deben cumplir con las leyes nacionales de transposición que rigen esta materia.

Según el Informe sobre la aplicación de la Directiva emitido por la Comisión de la UE, en relación con **este régimen sancionador** se detectaron algunos problemas de cumplimiento en relación con la transposición de la legislación nacional, por ejemplo, los siguientes:

- A. Falta de certeza jurídica sobre lo que constituye una conducta sancionable.
- B. Multas ineficaces y bajas, lo que reduce la disuasión.
- C. Penalización de las represalias únicamente contra las personas denunciantes, en lugar de ampliar la protección a otras categorías de personas, como los facilitadores (artículo 4 de la Directiva).

De acuerdo con **la legislación italiana**, una denuncia puede considerarse **inadmisibile** en los siguientes casos:

- A. cuando faltan datos que constituyan elementos esenciales de las denuncias (por ejemplo, los hechos denunciados y la Administración o Entidad en la que se han producido; la Administración o Entidad en cuyo contexto de trabajo opera la persona denunciante y el perfil profesional de esta última; una breve descripción de las formas en que la persona denunciante tuvo conocimiento de los hechos denunciados, etc.).
- B. cuando las violaciones denunciadas no se encuentran dentro del ámbito material definido por la ley italiana.

- C. cuando la persona informante no se encuentre entre las personas legalmente autorizadas para informar.
- D. cuando los hechos denunciados no se relacionen con el ámbito laboral.

2.6.1 ¿QUÉ OCURRE CUANDO LA DENUNCIA ES ADMITIDA A TRÁMITE?

El contenido de la denuncia está sujeta a la **verificación de la verosimilitud: todo lo que** no ofrece ninguna nota o elemento de falsedad puede definirse como plausible. Una denuncia se considera **verosímil** cuando hay **indicios suficientes para justificar nuevas investigaciones**. Llevar a cabo una evaluación exhaustiva de la plausibilidad es crucial para evitar investigaciones arbitrarias o innecesarias. La verosimilitud de una denuncia debe ser reevaluada continuamente a lo largo de la fase de investigación, asegurando que la evidencia recopilada se alinee con los hechos reportados. Posteriormente, se identifica a la persona presuntamente responsable y se recogen las pruebas.

Este es también el momento de **adoptar cualquier medida provisional con el fin de garantizar la eficacia** de la investigación y evitar daños que puedan ser irreparables en una etapa posterior. Estas medidas provisionales deberán planificarse en el procedimiento interno y de forma motivada y tras realizar un análisis previo de la necesidad y proporcionalidad de las mismas.

2.7 FACULTADES DE INVESTIGACIÓN

El objetivo principal de una investigación interna es reunir y preservar las pruebas necesarias para establecer los hechos y determinar las posibles responsabilidades. **Las investigaciones internas** no tienen el mismo alcance ni naturaleza jurídica que las investigaciones judiciales, ya que son de carácter administrativo. Toda recopilación de pruebas **debe evitar estrictamente** el uso de métodos ilegales, injustos o poco éticos que infrinjan **los derechos y libertades** fundamentales, tanto individuales como colectivos⁴⁴. Una investigación que no respete estos límites probatorios puede tener **graves consecuencias**, incluida la invalidación de las pruebas obtenidas y la **posible responsabilidad penal** de quienes llevan a cabo la investigación. Fundamentalmente, las investigaciones internas se basan en **diversos medios de verificación**, siendo los más comunes:

- A. documentación y/o información que incorpore datos y evidencias, y;
- B. entrevistas personales.

Para verificar la exactitud de los hechos reportados, los investigadores generalmente solicitan **documentos e informes** que contienen los datos necesarios como evidencia.

Estas fuentes de datos se pueden clasificar en:

- A. **Fuentes internas:** diversas unidades organizativas deben colaborar con la investigación, ya que pueden disponer de valiosos registros que aclaren las circunstancias del caso.

⁴⁴ Se recomienda consultar la sentencia del TEDH 2017/169399 de 5 de septiembre de 2017, caso *Bărbulescu c. Rumania* (*Barculescu II*) sobre el reconocimiento de la vida privada en el contexto laboral.

B Fuentes abiertas: entre las muchas que se pueden consultar, te sugerimos algunas:

- I.** Los datos sobre contratación pública pueden obtenerse consultando registros y plataformas con datos de contratación pública y en los portales de datos abiertos de las entidades del sector público.
- II.** Los datos comerciales pueden obtenerse en los registros mercantiles públicos y en los boletines oficiales.
- III.** En los portales de transparencia y datos abiertos de estas organizaciones se pueden encontrar datos de administraciones y entidades del sector público, como datos generales, presupuestos o cuentas anuales, cargos electos, gerentes y personal, organigramas, entre otros.
- IV.** Los datos relativos a ayudas y subvenciones se pueden obtener en los registros de subvenciones, portales de datos abiertos de diferentes entidades y también en boletines oficiales.
- V.** Los datos del censo electoral también se pueden obtener de fuentes abiertas.
- VI.** Datos del Registro de Grupos de Interés.
- VII.** Datos de las agendas de altos funcionarios.

Cuando se utilizan fuentes abiertas, es crucial **evaluar la fiabilidad de la información**. Los datos de código abierto a menudo deben filtrarse, validarse y verificarse para garantizar la precisión. **Una buena práctica para preservar la confidencialidad es no solicitar esa documentación a los departamentos o unidades de la propia organización si esa información se puede obtener consultando fuentes abiertas.**

2.7.1 ¿CUÁLES SON LAS RECOMENDACIONES RESPECTO A LA ENTREVISTA PERSONAL?

Se realizan las siguientes recomendaciones para el personal que se encargue de efectuar las entrevistas:

- A.** Realizar entrevistas con al menos dos investigadores presentes.
- B.** Prever las condiciones de discrecionalidad para entrevistar a las personas y cómo debe documentarse y grabarse la entrevista, así como proporcionar la información necesaria respecto al tratamiento de sus datos personales según lo establecido en el RGPD (art. 15 y siguientes).
- C.** La primera persona en ser entrevistada debe ser la persona denunciante (si no es anónima). A continuación, se debe continuar la entrevista con las personas que puedan tener información o hayan podido ser testigos de los hechos o conductas denunciadas y, por último, los posibles participantes y/o responsables de los hechos.
- D.** Prever si el entrevistado puede asistir en presencia de un abogado u otra persona (facilitador, representante sindical, etc.).

2.7.2 CIERRE DE UNA INVESTIGACIÓN INTERNA

Una investigación interna debe cerrarse cuando se considere infundada o infundada. Si se confirman los hechos denunciados, las posibles vías para **finalizar** la investigación interna son las siguientes:

- A. **Comunicación al departamento** o unidad competente para que adopte medidas para resolver la infracción denunciada, tales como, entre otras, medidas disciplinarias.
- B. **Traslado a una autoridad administrativa competente** cuando se confirme la infracción.
- C. **Traslado al Ministerio Público** y/u otra autoridad judicial, cuando los hechos denunciados integren un delito penal. Si la posible acción penal afecta a los intereses financieros de la Unión Europea, el informe se trasladará a la Fiscalía Europea.
- D. Recomendaciones internas en caso de haber detectado malas prácticas y falta de profesionalidad.

2.7.3 DE LA INVESTIGACIÓN INTERNA AL MINISTERIO PÚBLICO

La obligación de **trasladar información** de una investigación interna al **Ministerio Fiscal o a las autoridades judiciales** se ha incorporado a la transposición de la Directiva por parte de **España**. Sin embargo, esta disposición ha sido **controvertida**, en particular para **las personas jurídicas sujetas a responsabilidad penal empresarial**. En algunos casos, la obligación de informar podría entrar en conflicto con el derecho a no autoincriminarse de las personas jurídicas. Esto puede agregar complejidad a ciertas investigaciones y plantea retos legales. El **procedimiento de gestión** de denuncias debe prever la posibilidad de emitir **recomendaciones** para determinar el tratamiento que estas situaciones merecen y para ser insertadas en los procesos de mejora continua de la organización. De lo contrario, perdería su razón de ser un sistema que originalmente se concibe como una oportunidad para fortalecer también el sistema de integridad institucional y la cultura ética y de cumplimiento de la organización.

Las recomendaciones resultantes de una investigación interna pueden servir para diversos propósitos, tales como:

- A. Desarrollar programas de formación o sensibilización.
- B. Para mejorar los procesos o protocolos internos.
- C. Garantizar la correcta aplicación de las medidas correctivas.
- D. Informar al organismo de supervisión del cumplimiento sobre el cumplimiento del código de ética o conducta, etc.

Tanto **la persona afectada** por la denuncia como **la denunciante** deben ser **informadas del resultado de la investigación**. La Directiva reconoce el derecho de la persona informante a recibir información actualizada sobre el estado de su denuncia y a ser informado de los resultados finales de la investigación.

Es **recomendable que el informe o documento que concluya** las actuaciones incluya cómo se inició la investigación, el objeto de la misma, las actuaciones investigativas realizadas, quiénes han intervenido, la valoración de la exactitud de los hechos, así como las conclusiones y propuestas que **finalicen el seguimiento** del informe recibido con el fin de, tal y como establece la **Directiva**, para resolver la infracción denunciada. Debe ser, en todo caso, objetivo, imparcial, claro y preciso.

2.8 EL PAPEL DE LA AUTORIDAD INFORMANTE EXTERNA

2.8.1 LA IMPORTANCIA DE CONTAR CON CANALES EFICACES DE DENUNCIA DE IRREGULARIDADES

Según el considerando 63 de la Directiva, **la falta de confianza en la eficacia de los canales de denuncia** es uno de los principales factores que disuaden a los posibles informantes. Para abordar este problema, las autoridades competentes deben establecer canales de denuncia externos independientes y autónomos que garanticen un seguimiento diligente **de las denuncias** recibidas y proporcionen respuestas oportunas a las personas informantes. En los casos en que no existan canales internos, no hayan funcionado correctamente o cuando **las personas informantes temen represalias**, las autoridades competentes pueden estar mejor preparadas que las propias organizaciones para gestionar y hacer un seguimiento de las denuncias. **El artículo 11** de la Directiva establece que estos canales de denuncia externos deben ser independientes y autónomos en la recepción y tramitación de las denuncias relativas a infracciones legales. Además, **el considerando 65 hace hincapié en** que las autoridades competentes deben tener las capacidades y facultades necesarias para llevar a cabo un seguimiento adecuado, evaluar la exactitud de las denuncias, abordar las infracciones mediante investigaciones o enjuiciamientos, y adoptar las medidas correctivas necesarias. En caso necesario, **las autoridades también deben** poder remitir los casos a **otro organismo competente** para garantizar un seguimiento adecuado.

2.8.2 RETOS DE IMPLEMENTACIÓN Y PAPEL DE LAS AUTORIDADES COMPETENTES

La aplicación de la Directiva **se ha enfrentado a desafíos**, ya que algunos Estados miembros no han designado a las autoridades competentes con seguridad jurídica. Además, alrededor de la mitad de los Estados miembros **han transpuesto incorrectamente el artículo 11, apartado 6**, que establece las obligaciones de las autoridades que reciben denuncias, pero carece de competencia para tramitarlas. Por ejemplo, algunos Estados imponen estas obligaciones **sólo a autoridades específicas**, no garantizan la transmisión segura y oportuna de las denuncias u omiten el requisito de informar a la persona denunciante.

Cuando los canales de denuncia externos estén centralizados, los Estados miembros deben garantizar el cumplimiento de los requisitos de independencia y autonomía de la Directiva. Los artículos 12 y 18 de la Directiva establecen criterios estrictos para los canales de denuncia externos, incluida la garantía de la integridad y confidencialidad **de la información**, el almacenamiento a largo plazo y **la accesibilidad** para las denuncias escritas y orales, incluidas las presentaciones anónimas cuando lo permita la legislación nacional. **El artículo 13** exige a las autoridades competentes que publiquen información clara y accesible sobre los procedimientos de denuncia, los recursos, **la protección contra las represalias** y el asesoramiento confidencial para las personas informantes. Además, **se deben realizar revisiones periódicas** cada tres años para garantizar que los procedimientos de presentación de denuncias sigan siendo eficaces. Las autoridades competentes no solo gestionan **los canales**

externos, sino que también pueden **imponer sanciones** y desempeñar un papel vital en la promoción de una cultura que fomente la denuncia de irregularidades, garantizando que quienes denuncian irregularidades no sean estigmatizados ni se tomen represalias contra ellos.

2.8.3 DENUNCIAS SIMULTÁNEAS A CANALES INTERNOS Y EXTERNOS

Aunque la Directiva no exige que las personas informantes denuncien internamente antes de utilizar canales externos, no aborda explícitamente cómo gestionar las denuncias internas y externas simultáneas. Esta cuestión se debatió en la **cuarta reunión del grupo de expertos**, en la que se formularon recomendaciones para que los Estados miembros incluyeran disposiciones en sus leyes de transposición:

- A Las personas denunciantes deben esperar a que expire el período de tres meses antes de denunciar externamente.
- B Si optan por denunciar externamente antes de que finalice el período de tres meses, deben retirar su informe interno.

Además, las leyes nacionales podrían permitir a las autoridades pedir a las personas informantes su consentimiento para notificar a su empleador sobre su denuncia externa. Sin embargo, las personas informantes nunca perderían su protección por seguir estas recomendaciones.

Según la Comisión de la UE, en la práctica, la denuncia externa daría lugar a la retirada implícita de la denuncia interna. Si el empleador tiene conocimiento de una investigación externa, el canal interno ya no estaría obligado a hacer un seguimiento de la denuncia. Sin embargo, la organización aún puede optar por continuar con su investigación interna. Si las investigaciones internas y externas se llevan a cabo simultáneamente, las autoridades competentes siguen estando obligadas a investigar y abordar las violaciones en virtud de la Directiva.

En cualquier caso, las leyes de transposición deben abordar cómo abordar la concurrencia de denuncias a través del canal interno y del canal externo cuando la persona informante denuncia externamente antes de que haya expirado el plazo de tres meses para la investigación interna, siguiendo las recomendaciones formuladas por el grupo de expertos.

2.9 RECOMENDACIONES

1. PRESERVACIÓN DE LA CONFIDENCIALIDAD

Se deben implementar medidas procedimentales, técnicas, organizativas y de seguridad para preservar la confidencialidad de los datos personales contenidos en los canales internos de denuncia. Se debe hacer especial hincapié en garantizar y salvaguardar la confidencialidad de la identidad tanto de la persona informante como de las personas afectadas por la denuncia. Las investigaciones internas también deben llevarse a cabo de manera que se minimice el riesgo de violaciones de la confidencialidad a lo largo de todo el proceso.

2. PROCEDIMIENTOS DE SEGUIMIENTO

Los procedimientos de gestión y seguimiento de las denuncias internos deben ser detallados y abordados, además de los contenidos mínimos y principios previstos en las leyes de transposición, las diferentes fases del procedimiento de seguimiento de las denuncias de la forma más completa posible y especificando las actuaciones a realizar en cada una de ellas. También deben determinar cuáles serán los medios de verificación.

3. IDENTIFICACIÓN DE DENUNCIAS

Debe existir un sistema de identificación de denuncias, junto con un registro de las denuncias recibidas y las investigaciones realizadas. Esto garantiza la trazabilidad de las operaciones del canal interno y mejora la rendición de cuentas.

4. DETERMINAR LA ADMISIBILIDAD

El procedimiento de gestión de denuncias debe definir las circunstancias en las que una denuncia se considerará inadmisibile.

5. INVESTIGACIONES INTERNAS PLANIFICADAS

Las investigaciones internas deben planificarse adecuadamente, con un cronograma claro para evitar demoras indebidas que puedan exceder el marco de tiempo designado. El plan debe definir:

- A. El alcance de la investigación.
- B. Fuentes de evidencia y documentación requerida.
- C. Las personas involucradas y las que deben ser entrevistadas.

6. LÍMITES PROBATORIOS

La recogida de pruebas en las investigaciones internas debe respetar los límites probatorios y, en todo caso, debe respetar los derechos y principios fundamentales reconocidos en la Carta de los Derechos Fundamentales de la UE, así como las disposiciones de la legislación nacional y los procedimientos y protocolos internos aprobados por la organización.

7. MINIMIZAR LAS SOLICITUDES DE DOCUMENTOS Y RECORDAR LA CONFIDENCIALIDAD

No solicitar documentación a los servicios de la organización si esos datos pueden obtenerse de fuentes abiertas (por ejemplo, un nombramiento de un funcionario publicado en un boletín oficial), recordando también a las personas entrevistadas o a los servicios a los que se debe solicitar la información y/o documentación las obligaciones de confidencialidad y las consecuencias que puede conllevar una violación de la confidencialidad.

8. JUSTIFICACIÓN DE LA RECOPIACIÓN DE PRUEBAS EN LOS INFORMES

El informe de investigación debe incluir una justificación de las acciones y los métodos de verificación utilizados para recopilar pruebas.

9. PLANIFICACIÓN Y DOCUMENTACIÓN DE LA ENTREVISTA

Es necesario, en la etapa de planificación de la investigación, determinar los criterios para decidir qué personas deben ser entrevistadas y en qué orden, así como prever las condiciones de discrecionalidad para hacerlo y cómo debe documentarse y grabarse la entrevista. Es recomendable que lo lleven a cabo dos investigadores.

10. ESTRUCTURA DEL INFORME FINAL DE LA INVESTIGACIÓN

El informe que concluya la investigación debe incluir: cómo se inició la investigación, los objetivos de la investigación, las acciones tomadas y las personas involucradas, la evaluación de la exactitud de los hechos y las conclusiones y recomendaciones para resolver la irregularidad denunciada.

11. GARANTIZAR LA OBJETIVIDAD Y CLARIDAD EN LOS INFORMES

El **informe final** derivado de un procedimiento de denuncia debe redactarse con un enfoque **objetivo e imparcial**, basado exclusivamente en los hechos verificados y en las pruebas recabadas durante la investigación. Además, debe ser **claro, preciso y comprensible**, evitando tecnicismos innecesarios o ambigüedades que puedan dificultar su interpretación.

12. GESTIÓN DE CONFLICTOS DE INTERESES EN EL SEGUIMIENTO

El procedimiento de seguimiento debe incluir mecanismos para identificar, gestionar y mitigar los conflictos de interés entre los responsables del manejo de las denuncias.

13. RECOMENDACIONES PARA LA MEJORA ORGANIZATIVA

El procedimiento de gestión de denuncias debe permitir la posibilidad de emitir recomendaciones para determinar el tratamiento que merecen las situaciones detectadas de malas prácticas y falta de profesionalismo (irregularidades) y ser incluido en los procesos de mejora continua de la organización.

14. PRÓRROGA DE LOS PLAZOS DE INVESTIGACIÓN

Si una investigación no puede completarse dentro del período inicial de tres meses, se puede conceder una prórroga adicional de tres meses. Sin embargo, esta prórroga debe aprobarse antes de que finalice el primer período, justificar el motivo de la demora y especificar las acciones pendientes a completar.

15. PROMOCIÓN DE UNA CULTURA DE DENUNCIAS

Las autoridades competentes deben promover una cultura de denuncia de irregularidades.

16. MANEJO DE INFORMES EXTERNOS TEMPRANOS

Las leyes de transposición deben aclarar cómo tratar los casos en los que una persona denunciante informa externamente antes de que expire el período de otros tres meses de la investigación interna. Esto debe estar en consonancia con las recomendaciones del grupo de expertos de la Comisión Europea.

17. SANCIONES POR VIOLACIONES DE LA CONFIDENCIALIDAD

Sanciones disuasorias y efectivas por incumplimiento del requisito de confidencialidad que aborden específicamente el incumplimiento de esta disposición de la Directiva. Por lo tanto, en caso de violación de la confidencialidad y del deber de secreto, será necesario tener en cuenta los delitos tipificados en las leyes de transposición de los Estados miembros. En el caso de la Ley española de transposición⁴⁵, algunos delitos han sido tipificados como graves o muy graves cuando:

- A. La violación de las garantías de confidencialidad y anonimato previstas en la Ley, y en particular cualquier acción u omisión tendiente a revelar la identidad de la persona denunciante cuando haya optado por el anonimato, aun cuando no se produzca la divulgación efectiva de ésta.
- B. La violación del deber de secreto sobre cualquier aspecto relacionado con la denuncia. La mención que hace esta norma sobre la capacitación del personal con respecto a la confidencialidad es relevante, dado que la violación del deber de secreto, confidencialidad y anonimato puede constituir, como ya se ha mencionado, delitos específicos.

⁴⁵ Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre incumplimientos normativos y de lucha contra la corrupción.



Protección de datos personales



Capítulo 3

PROTECCIÓN DE DATOS PERSONALES

Capítulo 3

3.1 EL PAPEL DE LA PROTECCIÓN DE DATOS EN LOS SISTEMAS DE DENUNCIA DE IRREGULARIDADES

Dependiendo del **tipo de denuncia**, parte del **proceso de denuncia puede** implicar la recopilación, el uso y la divulgación de **datos personales**, lo que los sitúa en la intersección de los marcos de protección de datos y protección de las personas informantes. Garantizar que se respeten los principios de protección de datos y, al mismo tiempo, salvaguardar la confidencialidad y los derechos de las denunciantes es esencial para mantener la confianza y el cumplimiento legal. La protección de datos no es simplemente una obligación regulatoria, **es una herramienta diseñada para apoyar**, atender y abordar las necesidades de todas las partes involucradas en el proceso de denuncia. Lejos de ser un obstáculo para los flujos de trabajo de las organizaciones, los marcos sólidos de protección de datos **proporcionan claridad y estructura**, lo que garantiza que las personas informantes se sientan seguros a la hora de denunciar conductas indebidas y de buscar ayuda de los servicios de apoyo, al tiempo que salvaguardan los intereses de las organizaciones que reciben y gestionan dichas denuncias. Cuando se implementan de manera reflexiva, **las medidas de protección de datos pueden fomentar** una cultura de confianza, mejorar la transparencia y garantizar la integridad de los sistemas de denuncias internas.

El RGPD (Reglamento General de Protección de Datos), como piedra angular de la protección de datos en la Unión Europea, establece el marco legal para el tratamiento de datos personales y el equilibrio de los derechos y obligaciones de todas las partes interesadas (véase el **capítulo 1** para leer sobre la diferencia entre anonimato y confidencialidad). Los desafíos específicos del tratamiento de datos sensibles y personales en contextos de denuncia de irregularidades subrayan la importancia de alinear las estrategias de protección de datos con los requisitos de la Directiva sobre la protección de las personas informantes. A nivel nacional, los marcos para la protección de datos en los sistemas de denuncia de irregularidades requieren una planificación meticulosa y una alineación estratégica con los contextos legales y culturales nacionales.

La Organización de las Naciones Unidas (ONU) destaca que la protección efectiva de las personas informantes frente a posibles represalias es una piedra angular de la transparencia institucional y la rendición de cuentas⁴⁶.

⁴⁶ Protección contra las represalias - <https://www.un.org/en/ethics/protection-against-retaliation/index.shtml#:~:text=The%20UN's%20protection%20against%20retaliation,by%20any%20person%20that%20is>

Para que los mecanismos de denuncia resulten verdaderamente eficaces, deben centrarse en garantizar la confidencialidad y seguridad de quienes deciden informar sobre irregularidades, malas prácticas o actos de corrupción. Esta protección implica no solo el diseño de canales seguros de denuncia, sino también la posibilidad de mantener el anonimato y el uso de tecnologías avanzadas, como el cifrado de datos, que impidan la identificación no autorizada de las personas involucradas. **La política de “Protección contra represalias”** de la ONU sirve como ejemplo internacional de buenas prácticas, al resaltar el papel clave que desempeña la seguridad de la información en la creación de entornos institucionales donde los individuos se sientan seguros, respaldados y empoderados para denunciar sin temor a sufrir consecuencias negativas, ya sean personales, laborales o reputacionales. Promover esta cultura de protección es esencial para consolidar sistemas de integridad sólidos, confiables y sostenibles.

3.2 CONCEPTO PRINCIPAL Y PRINCIPIOS CLAVE DE LA PROTECCIÓN DE DATOS

La interacción entre el **Reglamento General de Protección de Datos** y la Directiva 2019/1937/UE sobre **personas informantes de irregularidades** establece el marco jurídico para garantizar que los datos personales se traten de forma legal, ética y transparente. Cuando los **principios de protección de datos** se incorporan en el diseño de los mecanismos de denuncia de irregularidades, mejoran su credibilidad y garantizan el cumplimiento de **las normas legales y éticas**.

3.2.1 ¿POR QUÉ LA PROTECCIÓN DE DATOS ES ESENCIAL PARA LA PROTECCIÓN DE LAS PERSONAS DENUNCIANTES?

- A. **Salvaguardar** la información personal, sensible y confidencial contra el uso indebido, robo, acceso no autorizado, etc.
- B. **Preserva la privacidad individual** al garantizar el control sobre los datos personales, reduciendo el riesgo de daño o explotación.
- C. **Prevenir el robo de identidad** y el fraude es un beneficio clave, ya que las violaciones que exponen información confidencial pueden tener consecuencias devastadoras. Las empresas también ganan confianza al priorizar la protección de datos, lo que fortalece las relaciones con los clientes y socios de protección de datos, ya que el incumplimiento puede dar lugar a graves multas y daños a la reputación.

Más allá de estos beneficios prácticos, la **protección de datos es una responsabilidad ética, que** fomenta la equidad y la transparencia en la forma en que se maneja la información. En un mundo interconectado, una seguridad de datos robusta también mitiga las amenazas de ciberseguridad, al priorizar la protección de datos, las personas y las organizaciones crean un entorno más seguro y confiable.

3.2.2 PRINCIPIOS CLAVE DE LA PROTECCIÓN DE DATOS

El principio de legalidad, equidad y transparencia exige que el procesamiento de datos se adhiera a los estándares legales y se lleve a cabo de manera transparente para mantener la confianza. Las organizaciones

deben comunicar claramente los fines de la recopilación de datos a los interesados, asegurándose de que se entiendan y respeten sus derechos. En resumen, los principios establecidos en el artículo 5 del RGPD⁴⁷ son el punto de partida para asegurar el cumplimiento de las normas de protección de datos y garantizar un entorno justo, transparente y seguro para las operaciones de tratamiento de datos:

- A. El **principio de legalidad, equidad y transparencia** subraya la importancia de procesar los datos personales de una manera que cumpla con la ley y respete los derechos de las personas afectadas. En el contexto de la denuncia de irregularidades, la legalidad exige que las organizaciones garanticen una base legal para el procesamiento de los datos, como el cumplimiento de una obligación legal o la búsqueda de intereses legítimos, como la investigación de conductas indebidas. Los datos también deben procesarse de manera justa, proporcionando transparencia, lo que requeriría que las organizaciones informen a los denunciantes sobre cómo se recopilarán, utilizarán, almacenarán y potencialmente compartirán sus datos, asegurándose de que comprendan las implicaciones de su divulgación.
- B. El **principio de limitación de la finalidad** dicta que los datos personales recopilados a través de los canales de denuncia solo deben utilizarse para los fines específicos para los que se recopilaron. Por ejemplo, si un/a denunciante denuncia acusaciones de fraude, la información proporcionada debe utilizarse estrictamente para investigar el problema denunciado y no para fines no relacionados como, por ejemplo, evaluar el rendimiento laboral de la persona informante. Este principio protege contra el uso indebido de los datos y garantiza que los derechos de las personas informantes y otras personas involucradas no se vean comprometidos injustamente.
- C. La **minimización de datos** es un principio clave que enfatiza la necesidad de recopilar solo los datos que son estrictamente necesarios para la investigación del asunto denunciado. La recopilación excesiva de datos no solo aumenta el riesgo de violaciones o usos indebidos, sino que también puede reducir la confianza que las personas informantes depositan en la confidencialidad del proceso de denuncia. Por ejemplo, los detalles sobre terceros o la identidad de la persona denunciante solo deben revelarse cuando sean absolutamente esenciales para la investigación y en cumplimiento de las leyes aplicables.
- D. El **principio de exactitud** garantiza que todos los datos personales tratados en el contexto de la denuncia de irregularidades sean correctos y estén actualizados. Los datos inexactos pueden dar lugar a resultados injustos, como acusaciones infundadas o la conclusión errónea de las investigaciones. Las organizaciones deben implementar procedimientos para verificar la exactitud de la información proporcionada por las personas informantes y para rectificar las inexactitudes con prontitud si se identifican.
- E. La **limitación del almacenamiento** requiere que los datos personales se conserven solo durante el tiempo necesario para cumplir con el propósito para el que se recopilaron. En los casos de denuncia de irregularidades, esto significa que los datos deben conservarse solo mientras dure la investigación y cualquier procedimiento legal o administrativo posterior. La retención de datos indefinidamente podría exponer a las personas a riesgos indebidos, como violaciones o usos

⁴⁷ Reglamento General de Protección de Datos - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

indebidos, y contravendría los principios de protección de datos establecidos.

F. Los **principios de integridad y confidencialidad** del RGPD son de suma importancia, por ejemplo, cuando en el caso de las personas informantes se puede proporcionar información muy sensible, y es responsabilidad de las organizaciones garantizar la seguridad de estos datos. Es esencial contar con medidas sólidas, como el cifrado, los controles de acceso y los canales de denuncia seguros, para evitar el acceso no autorizado, las violaciones de datos y otros riesgos que podrían comprometer la confidencialidad de las personas denunciantes o la integridad de las investigaciones.

G. El **principio de responsabilidad** exige que las organizaciones demuestren el cumplimiento de las leyes de protección de datos en su gestión de los casos de denuncia de irregularidades. Esto implica mantener registros de las actividades de procesamiento de datos, realizar evaluaciones de impacto de protección de datos para los sistemas de denuncia de irregularidades y garantizar que cualquier tercero involucrado en la investigación, como auditores o investigadores externos, se adhiera a las regulaciones de protección de datos relevantes. El Reglamento (UE) 2016/679 tiene en cuenta los requisitos de confidencialidad establecidos en otros actos jurídicos, tanto a nivel nacional como de la UE, y prevé que solo se debe contabilizar el tipo de datos, y no los datos en sí.

Además de estos principios básicos, la protección de las personas informantes también debe abordar consideraciones específicas como el anonimato, el equilibrio de derechos entre las personas denunciantes y las partes implicadas, y las transferencias transfronterizas de datos. Proporcionar canales de denuncia anónimos se alinea con el objetivo de proteger a los denunciantes de represalias. Al mismo tiempo, las organizaciones deben equilibrar la confidencialidad de las personas informantes con los derechos de las personas implicadas a acceder a la información relativa a las acusaciones formuladas en su contra, asegurándose de que esto se haga de acuerdo con los requisitos legales. Cuando la denuncia de irregularidades involucra asuntos internacionales, las organizaciones deben asegurarse de que cualquier transferencia transfronteriza de datos cumpla con la normativa aplicable, como el Reglamento General de Protección de Datos en la UE. Es crucial adherirse a estos principios para que las organizaciones puedan proteger los derechos de todas las partes involucradas, garantizar el cumplimiento de los marcos legales y fomentar una cultura de responsabilidad y transparencia en los sistemas de protección de denunciantes, y ayudar a cultivar la confianza.

3.3. BASE JURÍDICA PARA EL TRATAMIENTO LÍCITO DE DATOS PERSONALES

Artículo 6 del RGPD

Las organizaciones involucradas en los procesos de denuncia de irregularidades deben identificar una base legal para el procesamiento de datos personales, como se describe en el artículo 6 del GDPR⁴⁸. Las bases legales para el procesamiento incluyen el consentimiento, la necesidad

⁴⁸ Reglamento General de Protección de Datos - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

contractual, la obligación legal, los intereses vitales, el interés público y los intereses legítimos:

- A. **Consentimiento**, el tratamiento de datos personales es lícito cuando el interesado ha dado su consentimiento libre, específico, informado e inequívoco para que sus datos sean tratados para una finalidad determinada. El consentimiento debe ser claro, explícito (si se procesan datos sensibles) y fácilmente revocable en cualquier momento.
- B. La **base de la obligación contractual** se aplica cuando el tratamiento es necesario para cumplir un contrato en el que el interesado es parte o para tomar medidas precontractuales a petición del interesado. Esto garantiza que el tratamiento de datos esté directamente relacionado con el cumplimiento o la preparación de una obligación contractual (la protección de las personas informantes puede formar parte de las disposiciones de cualquier contrato).
- C. La **obligación legal** es lícita cuando es necesario para cumplir con un requisito legal específico impuesto al responsable del tratamiento. Esta base se suele utilizar cuando la legislación exige la retención, la notificación o el intercambio de datos (en virtud de actos legislativos, como la Directiva y la legislación nacional, la protección de las personas informantes está sujeta a obligaciones legales aplicables a las organizaciones).
- D. El **tratamiento** está justificado por motivos de interés vital cuando sea necesario para proteger la vida o la integridad física del interesado o de otra persona. A menudo se confía en esta base en emergencias, como situaciones médicas, en las que no se puede obtener el consentimiento.
- E. El **interés público o la autoridad oficial** se aplican cuando el tratamiento es necesario para llevar a cabo una tarea de interés público o en el ejercicio de la autoridad oficial conferida al responsable del tratamiento. Este es comúnmente utilizado por organismos públicos u organizaciones que operan bajo mandatos legales o gubernamentales, mientras que debe indicarse explícitamente en el acto legal en particular.
- F. **Intereses legítimos**, el tratamiento es lícito cuando es necesario para alcanzar los intereses legítimos del responsable del tratamiento o de un tercero, siempre que estos intereses no se vean anulados por los derechos y libertades del interesado. Esta base requiere una cuidadosa prueba de equilibrio para garantizar que el tratamiento no afecte injustamente a la privacidad del interesado (si bien la elección de la base jurídica más adecuada está en manos de las organizaciones, cuando sea posible, se recomienda basarse en la otra base jurídica prevista en el artículo 6 del RGPD).

En resumen, el tratamiento lícito de datos personales en virtud del artículo 6 del RGPD es esencial para garantizar el cumplimiento y fomentar la confianza en los mecanismos de denuncia de irregularidades. Las organizaciones deben determinar y documentar cuidadosamente la base jurídica adecuada, al tiempo que equilibran los derechos de los interesados y los requisitos establecidos en la Directiva.

Artículo 9 del RGPD

Las categorías especiales de datos personales, incluida la información relacionada con el origen racial o étnico, las opiniones políticas, las creencias

religiosas, la salud o la orientación sexual, están sujetas a mayores protecciones en virtud del artículo 9 del RGPD⁴⁹. Este tipo de datos se consideran sensibles y requieren condiciones específicas que justifiquen su tratamiento. El consentimiento explícito sigue siendo la base principal para el tratamiento de datos confidenciales, pero las organizaciones deben asegurarse de que dicho consentimiento se dé libremente y esté bien documentado.

PERSPECTIVA DE GÉNERO

Al integrar políticas sensibles al género en los **marcos de protección** de datos, los sistemas de denuncia de irregularidades pueden ser más seguros y eficaces, alentando a más personas, especialmente mujeres, a denunciar sin temor a represalias o exposición. Estas medidas son esenciales para garantizar que las denuncias de mala conducta basadas en el género se manejen de manera segura y que las identidades de las personas informantes permanezcan protegidas, especialmente cuando existen dinámicas de poder que podrían influir en el proceso. Se recomienda:

- A. Enfatizar cómo los sistemas de seguridad previenen las represalias en los casos basados en el género, asegurando que las denuncias estén protegidas para que las personas de la misma jerarquía en el lugar de trabajo, como supervisores o colegas, puedan acceder a ellos, para evitar posibles represalias.
- B. Garantizar que las plataformas que afirman el anonimato protejan realmente la identidad de la persona informante, en particular en los casos de desequilibrios de poder interseccionales y de género (por ejemplo, empleador-empleado, profesor-estudiante, gobierno-ciudadano).
- C. Proporcionar información explícita sobre cómo las medidas de seguridad digital (p. ej., TOR, pruebas de conocimiento cero, enmascaramiento de IP) protegen a las personas informantes que denuncian conductas indebidas basadas en el género.
- D. El desarrollo de plataformas en línea y líneas directas para denunciar la corrupción ofrece la ventaja de permitir que las personas hagan denuncias desde casa y, en algunos casos, de forma anónima. Esta forma de denunciar **puede ser especialmente conveniente para denunciar la violencia de género** vinculada a la corrupción y la sextorsión.

Estas medidas son esenciales para garantizar que las denuncias de mala conducta basadas en el género se manejen de manera segura y que las identidades de las personas informantes permanezcan protegidas, especialmente cuando existen dinámicas de poder que podrían influir en el proceso.

Protocolos de confidencialidad para las denuncias con perspectiva de género:

- A. Especificar protecciones de confidencialidad adicionales para las personas denunciantes que denuncien conductas indebidas basadas en el género, incluidas medidas para evitar la identificación indirecta a través de los detalles del caso.
- B. Detallar cómo se almacenarán de forma segura las denuncias de violencia de género y se separarán de las denuncias generales de mala conducta para minimizar la exposición.
- C. Aclare quién tiene acceso a las denuncias y cómo se aplica la protección de la identidad, asegurándose de que ninguna persona no autorizada (por ejemplo, colegas o superiores directos) pueda acceder a los datos confidenciales.
- D. La confidencialidad es clave para mantener la integridad de las denuncias de conductas indebidas basadas en el género y proteger a las personas informantes de posibles daños.

⁴⁹ Reglamento General de Protección de Datos - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

Otras bases legales para el procesamiento de datos confidenciales incluyen el cumplimiento de obligaciones legales, la necesidad del procesamiento para el interés público sustancial y la protección de intereses vitales. Por ejemplo, los casos de denuncia de irregularidades que involucran acusaciones de discriminación pueden requerir el procesamiento de datos confidenciales para fundamentar las reclamaciones o cumplir con las leyes contra la discriminación. Las organizaciones deben tener precaución e implementar salvaguardas adicionales al manejar dichos datos para mitigar los riesgos y garantizar el cumplimiento.

Derechos de los interesados en virtud del Reglamento (UE) 2016/79

El RGPD otorga a los interesados una serie de derechos diseñados para empoderar a las personas y proporcionar un mayor control sobre sus datos personales. Entre ellos se encuentran:

- A. El **derecho de acceso**, que permite a las personas obtener información detallada sobre el tratamiento de sus datos, incluidos los fines, las categorías, los destinatarios y los plazos de conservación.
- B. El **derecho de rectificación**, que garantiza que los datos inexactos o incompletos puedan corregirse con prontitud, mejorando la precisión y fiabilidad de la información procesada.
- C. El **derecho a solicitar** la supresión de los datos en circunstancias específicas, como cuando los datos ya no son necesarios para su finalidad original o cuando se retira el consentimiento. Sin embargo, este derecho no es absoluto y debe equilibrarse con la necesidad de conservar los datos con fines legales o de investigación.
- D. El **derecho a restringir el procesamiento**, que permite a las personas limitar el alcance de las actividades de procesamiento de datos, particularmente durante disputas sobre la exactitud o la legalidad del procesamiento.
- E. **Portabilidad de datos**, que permite a las personas recibir sus datos en un formato estructurado, de uso común y legible por máquina y transferirlos a otro responsable del tratamiento. Este derecho aumenta la autonomía individual y facilita la competencia entre los proveedores de servicios.
- F. El **derecho de oposición**, que permite a las personas impugnar las actividades de tratamiento de datos sobre la base de intereses legítimos o motivos de interés público. Las organizaciones deben evaluar cuidadosamente estas objeciones y proporcionar justificaciones claras para continuar o cesar las actividades de procesamiento.

Cada país determina los procedimientos específicos para que los interesados ejerzan sus derechos en virtud de los artículos 15 a 22 del RGPD⁵⁰, lo que suele incluir una solicitud al responsable del tratamiento para ejercer sus derechos. **La legislación nacional determina si dichas solicitudes deben presentarse** por vía electrónica, por escrito o ambas, o a través de un método específico para la organización, que no debe crear dificultades adicionales para los interesados, ni superar de manera desproporcionada la carga administrativa para el responsable del tratamiento.

⁵⁰ Reglamento General de Protección de Datos - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

3.6. INTERACCIÓN ENTRE EL MARCO JURÍDICO DE PROTECCIÓN DE DATOS PERSONALES Y LA DIRECTIVA 2019/1937/UE

Si bien el RGPD otorga a los interesados una amplia gama de derechos, siempre se debe tener en cuenta su interacción con otras legislaciones. **Cuando los interesados/as son considerados/as denunciantes** en virtud de la Directiva, **aún pueden ejercer cada uno de sus derechos en virtud del RGPD**, sin embargo, las organizaciones pueden negarse a llevar a cabo las solicitudes de los interesados para ejercer sus derechos, o negarse directamente, cuando esto violaría los requisitos legales para la protección de las personas informantes tanto en la Directiva como en la legislación nacional. Si bien el RGPD establece requisitos y plazos relacionados con la eliminación de datos, en este caso la persona que presenta el informe, o simplemente una vez finalizado el propósito para el que se recopilaban los datos, el Reglamento todavía se considera *lex generalis*. Con este fin, cuando existen diferentes períodos de retención para diferentes tipos de datos en la legislación nacional, se aplican sobre los establecidos por el GDPR. Además, las entidades aún pueden usar el **"interés legítimo"**, sin embargo, cuando hacerlo debe demostrarse con pruebas suficientes.

Ambos marcos comparten los objetivos comunes de fomentar la transparencia y la rendición de cuentas, salvaguardando al mismo tiempo los derechos de las personas. La gestión confidencial de las denuncias de irregularidades es un requisito fundamental en virtud de la Directiva y el RGPD. Ambos marcos exigen que sólo se reúnan y procesen los datos necesarios para alcanzar los objetivos del mecanismo de presentación de denuncias. Esto reduce los riesgos asociados con la recopilación excesiva y garantiza el cumplimiento del principio de limitación de la finalidad.

Los datos deben conservarse sólo durante el tiempo que sea necesario para investigar y resolver los problemas notificados. Por ejemplo, en **Italia**, la legislación nacional aplicable establece que las denuncias no pueden utilizarse más allá de lo necesario para darles un seguimiento adecuado. La identidad de la persona informante y cualquier otra información de la que pueda deducirse, directa o indirectamente, no podrán revelarse, sin su consentimiento expreso, a personas distintas de las competentes para recibir o dar seguimiento a las denuncias, expresamente autorizadas para tratar dichos datos de conformidad con el artículo 29 y el artículo 32, apartado 4, del Reglamento (UE) 2016/679⁵¹ (art. 12.1). También se prevé que los datos personales que manifiestamente no sean útiles para la tramitación de una denuncia específica no se recojan o, si se recogen accidentalmente, se eliminen inmediatamente (art. 13.2). Las denuncias internas y externas y la documentación relacionada se conservan durante el tiempo necesario para tramitar el informe y, en cualquier caso, no más de cinco años a partir de la fecha de comunicación del resultado final del procedimiento de notificación.

Las entidades públicas y privadas definen su propio modelo de recepción y gestión de denuncias internas, identificando las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado a los riesgos específicos derivados de los tratamientos realizados, sobre la

⁵¹ Reglamento General de Protección de Datos - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

base de una evaluación de impacto en materia de protección de datos. Además, **la legislación italiana de protección de datos** incluye una disposición específica para proteger la confidencialidad de la identidad de la persona informante (art. 2-undecies en el Decreto Legislativo n.º 196 del 30 de junio de 2003. Este artículo fue introducido con el Decreto Legislativo n.º 101 del 10 de agosto de 2018, para cumplir con el Reglamento (UE) n.º 2016/679). La citada disposición establece que en el contexto de una denuncia, el sujeto afectado, presunto autor de la infracción, con referencia a sus datos personales tratados por la Administración, no puede ejercer los derechos previstos en los artículos 15 a 22 del Reglamento (UE) n.º 2016/679, ya que el ejercicio de tales derechos podría resultar perjudicial para la protección de la confidencialidad de la identidad del/la denunciante. La ley prevé la posibilidad de que la persona afectada solicite a la Autoridad de Protección de Datos controles sobre la conformidad del tratamiento de sus datos. La Autoridad de Protección de Datos proporciona comentarios sobre el resultado relativo.

Al alinear las estrategias de protección de datos con los requisitos de la Directiva sobre informantes:

- A Las **organizaciones** pueden crear sistemas integrados que respeten los derechos individuales y, al mismo tiempo, apoyen una gobernanza y un cumplimiento eficaces. Las personas informantes se sienten seguros al presentarse, sabiendo que sus datos personales serán tratados con el máximo cuidado.
- B Se fortalece la **confianza del público** en los sistemas de presentación de denuncias.
- C Los **reguladores** y las organizaciones deben trabajar en colaboración para garantizar una implementación sin problemas, aprovechando herramientas como protocolos de denuncias estandarizados, pautas claras de retención de datos y técnicas de anonimización accesibles.

3.8 PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO EN LOS CANALES INTERNOS DE DENUNCIA

Las organizaciones pueden crear sistemas de denuncia de irregularidades sólidos que se alineen con los principios de protección de datos desde el diseño y por defecto.

3.8.1 ¿QUÉ ES LA PROTECCIÓN DE DATOS DESDE EL DISEÑO?

Canal de denuncia interna: Incorporación de medidas de seguridad y consideraciones de privacidad en el desarrollo de mecanismos de denuncia. Por ejemplo, los sistemas deben incluir características como canales de comunicación cifrados, controles de acceso basados en roles y registros de auditoría para garantizar la confidencialidad y la responsabilidad. La minimización de datos debe guiar el diseño de los formularios de denuncias y los flujos de trabajo, asegurando que solo se recopile la información esencial durante el informe inicial. Las organizaciones también deben implementar procedimientos para verificar la exactitud y pertinencia de los datos recopilados, salvaguardando al mismo tiempo el anonimato de los las personas informantes. Un ejemplo de ello sería el desarrollo de mecanismos internos que permitan la verificación cruzada de tipos específicos de datos,

sin revelar la identidad de la persona informante, con el fin de demostrar la validez de las afirmaciones hechas en las denuncias presentadas. Ya existen soluciones de software (incluidos los softwares utilizados por los analistas de datos) que permiten que diferentes bases de datos (departamentos específicos, RRHH, etc.) crucifiquen dicha información en formato anónimo.

Un estudio de caso de Italia: La implementación de sistemas de software que incorporan un cifrado robusto para garantizar la confidencialidad en los canales de denuncia externos es un punto de referencia para una protección de datos eficaz desde el diseño. Un ejemplo es Globaleaks, que crea un identificador para cada denunciante, lo que permite una comunicación asíncrona y segura con el canal de denuncias. Esta práctica garantiza que ninguna de las partes pueda acceder a datos personales innecesarios, cumpliendo así el principio de minimización de datos.

3.8.2 ¿QUÉ ES LA PROTECCIÓN DE DATOS POR DEFECTO?

CP. 1 ➤

La necesidad de que las organizaciones procesen solo los datos necesarios para fines específicos. Los sistemas de denuncias internos deben aplicar automáticamente la configuración de privacidad más alta y limitar el acceso a los datos al personal designado. Las evaluaciones periódicas de las configuraciones y prácticas del sistema garantizan que estos principios se apliquen y actualicen de forma coherente para hacer frente a los riesgos emergentes y a los cambios normativos. Para reforzar la protección de datos, las organizaciones deben adoptar tecnologías innovadoras, como las comprobaciones automatizadas de cumplimiento, la detección de anomalías en tiempo real en los flujos de datos y las soluciones de almacenamiento cifrado (véase el [Capítulo 1](#) para obtener más información). El compromiso con los empleados a través de talleres o formación sobre protección de datos y sistemas de denuncias internos puede cerrar la brecha entre la tecnología y la aplicación práctica. Este enfoque holístico garantiza que el personal de todos los niveles comprenda sus responsabilidades, fomentando una cultura de protección de datos proactiva.

3.9. PROTECCIÓN DE DATOS EN CANALES DE DENUNCIA EXTERNOS

Los canales de denuncia externos, como los gestionados por los organismos reguladores, se enfrentan a retos adicionales a la hora de equilibrar la transparencia con la protección de datos. **Los canales de comunicación seguros** son esenciales para proteger la integridad de las denuncias y evitar el acceso no autorizado a información confidencial. Las organizaciones que operan canales externos deben establecer políticas claras **que describan el manejo de los datos personales**, incluidos los procedimientos para verificar la autenticidad de las denuncias y proteger las identidades de los denunciantes.

La transparencia es clave; Las personas informantes deben disponer de opciones de anonimato, con mecanismos para una comunicación de seguimiento segura. La protección proporcionada a los y las denunciantes se encuentra dentro de los fines legítimos en virtud del RGPD, ya que proporcionar información a una persona objeto de una denuncia

presentada mientras la investigación está en curso puede corromper la propia investigación al conducir a la identificación de la persona denunciante. El uso de sistemas seguros y auditables puede garantizar la responsabilidad y el cumplimiento de los requisitos de protección de datos. Los organismos reguladores también deben considerar la implementación de controles de acceso de múltiples capas y protocolos de cifrado sólidos para proteger la información confidencial. Las auditorías periódicas de terceros de estos sistemas proporcionan una capa adicional de garantía de que se respetan los principios de protección de datos. Para garantizar la confianza del público, los canales de denuncia externos también deben hacer hincapié en la equidad y la imparcialidad. Estas medidas demuestran un compromiso tanto con la protección de datos como con la rendición de cuentas, reforzando la confianza en los sistemas de información externos.

3.9.1 BUENAS PRÁCTICAS DE ITALIA

Para cumplir con todos los requisitos del RGPD mencionados anteriormente, en **Italia**, el Decreto Legislativo 24/2023 establece que las denuncias no se pueden utilizar más allá de lo necesario para hacer un seguimiento adecuado de los mismos. La identidad de la persona informante y cualquier otra información de la que pueda deducirse, directa o indirectamente, no podrán revelarse, sin su consentimiento expreso, a personas distintas de las competentes para recibir o dar seguimiento a las denuncias, expresamente autorizadas para tratar dichos datos de conformidad con el artículo 29 y el artículo 32, apartado 4, del Reglamento (UE) 2016/679⁵² (art. 12.1). También se prevé que los datos personales que manifiestamente no sean útiles para la tramitación de una denuncia específica no se recojan o, si se recogen accidentalmente, se eliminen inmediatamente (art. 13.2).

Las denuncias internas y externas y la documentación relacionada se conservan durante el tiempo necesario para procesar el informe y, en cualquier caso, no más de cinco años a partir de la fecha de comunicación del resultado final del procedimiento de informe, de acuerdo con una disposición específica de **la legislación italiana de protección de datos** (art. 2-undecies en el Decreto Legislativo n.º 196 del 30 de junio de 2003, introducida con el Decreto Legislativo n.º 101 del 10 de agosto de 2018).

3.9.2 MITIGACIÓN DE LOS RIESGOS REPUTACIONALES

Los canales de denuncia externos también se enfrentan a mayores riesgos de reputación cuando la información sensible se hace pública, como subrayan los encuestados italianos. Las divulgaciones de los empleados a través de las redes sociales, por ejemplo, pueden dañar significativamente la reputación de una empresa o autoridad pública. La implementación de políticas estrictas sobre la divulgación pública y la promoción de canales de denuncia externos seguros pueden mitigar estos riesgos. El artículo 11-ter del Código de Conducta italiano subraya esta cuestión, demostrando la necesidad de armonización entre las legislaciones nacionales y las disposiciones de la Directiva. Para contrarrestar los riesgos para la reputación y cumplir los principios de la Directiva, las organizaciones

⁵² Reglamento General de Protección de Datos - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

pueden ofrecer múltiples vías de denuncia seguras y oficiales, incluidas líneas directas anónimas y plataformas en línea cifradas. Estos canales pueden evitar que las personas informantes recurran a las redes sociales, manteniendo así la confidencialidad y limitando el daño a la reputación.

3.9.3 EXPERIENCIA Y FORMACIÓN

Los comentarios de las entrevistas españolas ponen de manifiesto la importancia crítica de la experiencia en materia de protección de datos. Las organizaciones deben asegurarse de que el personal que opera los canales de denuncia externos esté adecuadamente capacitado y posea un conocimiento profundo de los requisitos del GDPR. Los talleres y programas de certificación periódicos para los Delegados de Protección de Datos (DPO) y otro personal relevante pueden reforzar el cumplimiento y fomentar una cultura que priorice la privacidad. Con la implementación de estas medidas, los canales de denuncia externos pueden cumplir el doble objetivo de promover la transparencia y salvaguardar los derechos de todas las partes implicadas, fomentando la confianza y el cumplimiento legal.

3.10. MEDIDAS TÉCNICAS Y ORGANIZATIVAS

La implementación de medidas técnicas y organizativas sólidas es esencial para garantizar el cumplimiento del RGPD⁵³ y salvaguardar los datos personales. El cifrado y la seudonimización son técnicas ampliamente reconocidas que mejoran la seguridad de los datos al hacer que los datos sean ininteligibles para partes no autorizadas. Los controles de acceso basados en roles limitan el acceso a los datos al personal autorizado, lo que reduce el riesgo de divulgaciones no autorizadas.

Las organizaciones deben desarrollar e implementar políticas integrales de protección de datos que describan las funciones, responsabilidades y procedimientos para el manejo de datos personales. Los programas periódicos de formación y concienciación para los empleados garantizan que todas las partes interesadas comprendan sus obligaciones en virtud del RGPD y de los marcos de protección de las personas informantes. Las auditorías periódicas y las evaluaciones de riesgos ayudan a identificar las vulnerabilidades y a garantizar que las medidas de seguridad sigan siendo eficaces y estén actualizadas.

Los planes de respuesta a incidentes son importantes para abordar las filtraciones de datos y minimizar su impacto. Las organizaciones deben establecer protocolos claros para detectar, informar y mitigar las infracciones, así como notificar a las personas y autoridades afectadas cuando sea necesario.

3.11. PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO EN LA DIVULGACIÓN PÚBLICA

La divulgación pública presenta desafíos únicos para equilibrar la protección de datos con la necesidad de transparencia y rendición de cuentas. La forma en que las organizaciones mantienen sus obligaciones de

⁵³ Reglamento General de Protección de Datos (Artículo 24) - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

protección de las personas informantes en estos casos es esencial. De hecho, la divulgación pública representa la forma más sensible de denuncia de irregularidades, donde el potencial de daño a la reputación y las implicaciones legales son más altas. Con arreglo a la Directiva, la divulgación pública se considera un último recurso, admisible solo cuando se han agotado los canales de denuncia internos y externos o se consideran ineficaces. Antes de divulgar información al público, las organizaciones (ya sea en el papel de canales de denuncia externos o internos) deben evaluar cuidadosamente si la divulgación se alinea con los principios del GDPR y sirve al interés público. Siempre que sea posible, se debe obtener el consentimiento explícito, especialmente cuando se trata de datos personales sensibles.

3.11.1 EL PAPEL DE LA PROTECCIÓN DE DATOS EN LAS DIVULGACIONES PÚBLICAS

En el contexto de las divulgaciones públicas, las organizaciones y las personas informantes deben navegar cuidadosamente por la delgada línea entre la transparencia y el daño a la reputación. Los protocolos de redacción desempeñan un papel fundamental en la protección de la privacidad durante las divulgaciones públicas. Las organizaciones deben eliminar u ocultar los datos personales que no sean esenciales para lograr el propósito de la divulgación. Esto garantiza el cumplimiento del principio de minimización de datos, al tiempo que salvaguarda los derechos de las personas. El software italiano GlobaLeaks antes mencionado ejemplifica cómo la tecnología puede respaldar las divulgaciones públicas. Al anonimizar y cifrar las comunicaciones, estas plataformas permiten a las personas denunciantes compartir información de forma segura, lo que reduce los riesgos asociados a las divulgaciones públicas no reguladas. La incorporación de dicha tecnología en los marcos de divulgación pública puede garantizar el cumplimiento de la Directiva, manteniendo al mismo tiempo la confianza de la persona informante.

Desde **Italia** se ha planteado una preocupación por el posible uso indebido de las divulgaciones públicas a través de las redes sociales. Cuando las personas informantes eluden los mecanismos formales de denuncia y revelan información confidencial en plataformas abiertas, no solo ponen en peligro su confidencialidad, sino que también plantean riesgos significativos para la reputación corporativa o institucional.

Las organizaciones deben informar a los empleados sobre los límites legales de las divulgaciones públicas. El artículo 11 b del Código de Conducta italiano, por ejemplo, aborda el uso descuidado de las redes sociales y enfatiza la importancia de adherirse a mecanismos estructurados de denuncia. Complementar estas medidas con canales internos y externos accesibles y sólidos puede reducir la probabilidad de que las personas informantes recurran a plataformas públicas. Sin embargo, en **Italia** sigue habiendo un desajuste entre las disposiciones del Código de Conducta y el Decreto Legislativo 24/2023 sobre la denuncia de irregularidades. Este último reconoce explícitamente la posibilidad de divulgación pública bajo ciertas condiciones, un matiz que no se refleja adecuadamente en el Código. Al mismo tiempo, la falta de alineación entre el Código de Conducta y el marco legislativo vigente genera confusión en cuanto al destinatario de las denuncias internas, ya que sigue identificando incorrectamente al superior

jerárquico en lugar del Responsable de Prevención de la Corrupción y la Transparencia.

3.11.2 ¿CÓMO MEJORAR LA SEGURIDAD EN LAS DIVULGACIONES PÚBLICAS?

Para alinear las divulgaciones públicas con los principios de protección de datos, las organizaciones y los organismos de supervisión deben desarrollar directrices y medidas de protección claras. Las partes interesadas españolas han destacado la importancia de salvaguardar la identidad del/la denunciante incluso en las divulgaciones públicas.

La perspectiva búlgara hace hincapié en la importancia de limitar el acceso a las denuncias al personal esencial. Aplicando el mismo principio a las divulgaciones públicas, los organismos de supervisión pueden redactar información confidencial que no sea crítica para el interés público, equilibrando la transparencia con la protección de datos.

Para evitar la mala gestión de datos cuando se realiza una divulgación pública, recomendamos que los organismos reguladores implementen medidas estrictas para evitar el mal manejo de los datos, como:

- A. Establecer protocolos para verificar la exactitud de la información reportada;
- B. Documentar todas las acciones tomadas en respuesta a la divulgación.

Una comunicación clara y transparente sobre los procesos de denuncia y sus garantías genera tranquilidad entre las partes interesadas, ya que demuestra que el sistema es justo, accesible y respetuoso con los derechos de todos. Esta transparencia fortalece la confianza institucional y promueve una cultura organizativa basada en la integridad y la rendición de cuentas.

3.12. CENTRO(S) DE INFORMACIÓN Y PROTECCIÓN DE DATOS ORGANIZADOS POR LA SOCIEDAD CIVIL: UNA CUESTIÓN ABIERTA

CP. 4➔

El artículo 20 de la Directiva⁵⁴ reconoce el papel de los "centros de información" como servicios de apoyo que la sociedad civil puede organizar y poner a disposición para ayudar a los y las posibles denunciantes durante la fase de dilemas éticos y dudas generales sobre el funcionamiento del sistema. La ley establece que esta función también puede ser desempeñada por instituciones especializadas.

Para cumplir esta función (véase el **capítulo 4**), estos centros de información entran necesariamente en contacto, gestionan y almacenan datos personales, así como otra información sensible.

A este respecto, la disposición inicial N° 89 de la Directiva establece que los centros de información **"están obligados a mantener la confidencialidad de la información recibida"**.

⁵⁴ Directiva (UE) 2019/1937 - <https://eur-lex.europa.eu/eli/dir/2019/1937/oj/eng>

Sin embargo, la Directiva no proporciona más detalles sobre cómo cumplir con este deber, si estos centros deben equipararse a las instituciones informantes o si deben aplicarse condiciones especiales. **La Directiva sigue siendo vaga en este punto.** Esta laguna no se ha abordado suficientemente en las normativas de varios países, sobre todo teniendo en cuenta que, salvo raras excepciones, estos servicios de apoyo aún no se practican ampliamente en toda Europa.

En ausencia de directrices específicas sobre las prácticas de tratamiento de datos, existe el **riesgo de que se impida a los servicios de apoyo el tratamiento de datos**, lo que limitaría su capacidad para funcionar (y podría poner en peligro su capacidad para operar), al tiempo que restringía el acceso de los y las posibles denunciantes al apoyo.

La normativa nacional, o las directrices proporcionadas por las autoridades pertinentes en materia de denuncia de irregularidades, deben tratar de colmar esta laguna mediante el establecimiento de protocolos claros de tratamiento de datos que permitan a las personas denunciantes recibir apoyo, al tiempo que exigen a los centros de información que apliquen sistemas de cifrado sólidos para recibir, almacenar (durante un período limitado) y compartir datos entre los operadores, garantizando de la mejor manera posible la protección y la confidencialidad de la información de la persona denunciante. Tal como se establece en el considerando 74 de la Directiva, los miembros del personal de las autoridades competentes responsables de la tramitación de las denuncias deben recibir una formación profesional, en particular sobre las normas aplicables en materia de protección de datos, con el fin de tramitar las denuncias y garantizar la comunicación con la persona informante, así como para hacer un seguimiento adecuado de la misma.

PERSPECTIVA DE GOBIERNO ABIERTO

Las estrategias sólidas de protección de datos son primordiales para una gran cantidad de partes interesadas, como las personas informantes, los gestores de los canales de denuncia, las entidades que ofrecen apoyo a los posibles denunciantes, como las OSC, y las partes interesadas que tienen un papel como canal de divulgación pública, como los periodistas y los medios de comunicación. Estas estrategias deben incluir mecanismos seguros para el manejo de información confidencial a fin de salvaguardar la identidad y los intereses de las personas informantes. **La colaboración intersectorial** con la participación de los reguladores nacionales, los responsables de la protección de datos y los responsables políticos puede ser decisiva en el desarrollo de soluciones innovadoras de **protección de datos adaptadas a diversos escenarios de denuncia de irregularidades, especialmente para abordar las complejidades de las divulgaciones públicas.** Los esfuerzos conjuntos pueden armonizar las legislaciones nacionales con las disposiciones de la Directiva, desarrollando directrices claras sobre el uso ético de los datos para ayudar a todas las partes interesadas a mantener la transparencia respetando al mismo tiempo la privacidad.

Una cuestión cada vez más crítica que debe abordarse en el marco de un gobierno abierto es el **tratamiento de datos sensibles y personales por parte de las entidades asesoras y de apoyo**, tanto cívicas como institucionales, tal y como reconoce la Directiva. La propia Directiva (en sus disposiciones iniciales 89 y 90) obliga a estas entidades a garantizar un tratamiento eficaz de los datos, aunque no proporciona más detalles.

Los servicios de apoyo y asesoramiento, en su función de orientar a los y las posibles denunciantes, entran inevitablemente en contacto con datos sensibles. Su propósito no es simplemente proporcionar información genérica y descontextualizada, sino más bien ayudar a las personas a navegar por los canales de denuncia adecuados de una manera significativa. Un enfoque puramente neutral e imparcial no satisfaría las necesidades de las potenciales personas informantes.

Este tema debe discutirse abiertamente dentro de un entorno de gobierno abierto, a través del desarrollo de directrices claras, mediante la organización de debates conjuntos en los que participen las autoridades de protección de datos, los representantes de las organizaciones de apoyo (tanto cívicas como institucionales) y los organismos reguladores de denuncia de irregularidades.

El objetivo debe ser lograr el equilibrio adecuado entre dos necesidades clave: garantizar que las potenciales personas informantes reciban una orientación significativa (lo que puede requerir cierto nivel de tratamiento de datos por parte de los servicios de apoyo) y, al mismo tiempo, salvaguardar sus datos personales.

Por ejemplo, las discusiones deben establecer:

- A. Políticas de retención claras, incluido un período máximo de almacenamiento para datos confidenciales.
- B. Métodos seguros y confidenciales para el intercambio de datos entre las potenciales personas informantes y los servicios de apoyo.
- C. Protocolos de comunicación definidos entre asesores dentro de un mismo servicio.

Una interpretación restrictiva que priorice la privacidad por encima de todo lo demás podría socavar involuntariamente los propios intereses de las potenciales personas informantes al limitar su capacidad para buscar orientación eficaz.

3.13 RECOMENDACIONES

La Fundación Konrad Adenauer (KAF), a lo largo de su trabajo en diversos proyectos y políticas, enfatiza que los marcos legales integrales (similares al GDPR)⁵⁵ son esenciales para fomentar la transparencia al tiempo que se salvaguardan los derechos individuales, definiendo claramente el alcance y los límites de las actividades de denuncia de irregularidades. KAF aboga por mecanismos que defiendan el principio de proporcionalidad en el tratamiento de datos, equilibrando la necesidad de investigar las conductas indebidas denunciadas con el derecho a la privacidad de todas las personas implicadas. También destacan la importancia de las campañas de concienciación pública para educar a los ciudadanos y las organizaciones sobre sus derechos y responsabilidades dentro de los marcos de denuncia de irregularidades. Se han enumerado algunos consejos prácticos para la implementación de políticas de protección de datos⁵⁶:

⁵⁵ Ver: https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_47778_2.pdf/c2a538a2-ed3d-1aa7-b2ae-2736329c8a66?version=1.0&t=1539649646584

⁵⁶ Transparencia y rendición de cuentas- <https://www.kas.de/en/web/rspno/veranstaltungsberichte/detail/-/content/transparenz-und-rechenschaftspflicht>

1. ESTABLECIMIENTO DE ÓRGANOS DE SUPERVISIÓN INDEPENDIENTES

El establecimiento de órganos de supervisión independientes para supervisar la aplicación de los mecanismos de denuncia de irregularidades, tal como se define en el marco jurídico nacional aplicable.

2. AUTORIDAD DE LOS ÓRGANOS DE SUPERVISIÓN

Estos organismos deben tener autoridad para investigar quejas, revisar las prácticas de protección de datos y garantizar el cumplimiento de las normas legales, cuando se refieran a autoridades independientes que reciban quejas a través de un canal externo (o su canal interno).

3. IMPORTANCIA DE LA FORMACIÓN EN DENUNCIA Y PROTECCIÓN DE DATOS

Los programas de formación para los empleados del sector público y privado son cruciales para crear conciencia sobre los protocolos de denuncia de irregularidades y los principios de protección de datos.

4. MANEJO CONFIDENCIAL DE DENUNCIAS POR PARTE DE LOS EMPLEADOS

Los empleados deben estar equipados para reconocer la importancia de la confidencialidad, manejar de forma segura las denuncias confidenciales y evitar divulgaciones no autorizadas.

5. BUENAS PRÁCTICAS PARA FORTALECER EL CUMPLIMIENTO

En general, aquí hay varias buenas prácticas que las organizaciones pueden seguir para fortalecer su cumplimiento y fomentar la confianza:

5.1 DESARROLLO DE POLÍTICAS DETALLADAS DE DENUNCIA

Las organizaciones deben desarrollar políticas detalladas que describan el propósito, el alcance y los procedimientos de sus sistemas de denuncia de irregularidades. Estas políticas deben abordar los requisitos de protección de datos, incluida la recopilación, el almacenamiento, el procesamiento y la retención de datos. Al hacer que estas políticas sean accesibles para todas las partes interesadas, las organizaciones demuestran transparencia y responsabilidad.

5.2 NOMBRAMIENTO DE UN RESPONSABLE DE PROTECCIÓN DE DATOS (DPO)

El nombramiento de un responsable de protección de datos cualificado es fundamental para garantizar el cumplimiento continuo del RGPD y de la Directiva sobre informantes. Los DPO pueden proporcionar orientación sobre el manejo de datos personales, realizar auditorías y servir como punto de contacto para los interesados y las autoridades supervisoras.

5.3 PROGRAMAS DE CAPACITACIÓN ADAPTADOS A LOS GRUPOS DE INTERÉS

Los programas de capacitación deben adaptarse a las necesidades de los diferentes grupos de partes interesadas, incluidos los empleados, los gerentes y los proveedores de servicios externos. Estos programas deben enfatizar la importancia de la confidencialidad, la minimización de los datos y los derechos de los interesados. La capacitación basada en escenarios puede ayudar a los empleados a comprender cómo manejar los casos delicados de denuncia de irregularidades de manera efectiva.

5.4 IMPLEMENTACIÓN DE CANALES SEGUROS DE DENUNCIA

Las organizaciones deben implementar canales de denuncia seguros y fáciles de usar que permitan a las personas informantes enviar información de forma confidencial. La autenticación multifactor y los protocolos de comunicación cifrados pueden mejorar la seguridad de estos sistemas. Además, las organizaciones deben probar estos sistemas con regularidad para identificar y abordar las vulnerabilidades.

5.5 SEGUIMIENTO Y AUDITORÍAS PERIÓDICAS DE LOS SISTEMAS

El seguimiento y la auditoría periódicos de los sistemas de denuncia de irregularidades ayudan a garantizar el cumplimiento de los requisitos de protección de datos. Las organizaciones deben mantener registros detallados de las actividades de procesamiento de datos, incluidas las justificaciones para la recopilación y retención de datos. Las auditorías pueden identificar brechas en el cumplimiento y proporcionar oportunidades para la mejora continua.

5.6 COLABORACIÓN CON AUTORIDADES Y ORGANISMOS REGULADORES

Colaborar con las autoridades nacionales de protección de datos y otros organismos reguladores puede ayudar a las organizaciones a mantenerse informadas sobre los cambios en la legislación y las mejores prácticas. La colaboración también facilita la resolución de casos complejos, como los relacionados con transferencias transfronterizas de datos o conflictos entre las normativas nacionales y de la UE.

5.7 USO DE TECNOLOGÍAS INNOVADORAS CONFORMES AL RGPD

Las tecnologías innovadoras, como la inteligencia artificial y el aprendizaje automático, podrían mejorar la eficiencia y la seguridad de los sistemas de denuncia de irregularidades. Por ejemplo, las herramientas impulsadas por IA pueden detectar patrones de mala conducta, identificar violaciones de datos y respaldar procesos de anonimización. Sin embargo, las organizaciones deben asegurarse de que estas tecnologías cumplan con el RGPD y otras regulaciones aplicables.

5.8 ESTABLECIMIENTO DE MÉTRICAS DE EFICACIA

Las organizaciones deben establecer métricas para evaluar la eficacia de sus sistemas de denuncia, incluida la tasa de resolución de los casos

denunciados, los niveles de satisfacción de las personas informantes y el cumplimiento general de la organización con los estándares de protección de datos. Los informes periódicos sobre estas métricas pueden generar confianza entre las partes interesadas y destacar las áreas de mejora (véase el [capítulo 5](#) para obtener más información).

5.9 FOMENTO DE UNA CULTURA DE MEJORA CONTINUA

La protección de datos es un proceso continuo que requiere que las organizaciones se adapten a los cambiantes panoramas legales, tecnológicos y sociales. Al fomentar una cultura de mejora continua, las organizaciones pueden garantizar que sus sistemas de denuncia de irregularidades sigan siendo eficaces, seguros y cumplan con los estándares en evolución. Al incorporar estas estrategias/buenas prácticas, las organizaciones y los gobiernos nacionales pueden establecer mecanismos de denuncia de irregularidades que cumplan con la ley y sean efectivos en la práctica. Estos sistemas no solo alientan a las personas a denunciar conductas indebidas con confianza, sino que también fortalecen la gobernanza general, mejoran la confianza pública y contribuyen a una cultura de integridad.

5.10 EVALUACIÓN DE PROPORCIONALIDAD EN DIVULGACIONES PÚBLICAS

Equilibrar el interés público con los derechos a la privacidad requiere una evaluación de proporcionalidad, teniendo en cuenta factores como la gravedad del problema denunciado, el impacto potencial de la divulgación y la disponibilidad de soluciones alternativas. Las organizaciones deben documentar sus procesos de toma de decisiones para demostrar la responsabilidad y el cumplimiento de los requisitos reglamentarios, como los registros internos, las normas y procedimientos, los códigos de conducta y los códigos de ética.

5.11 PRIORIDAD A LA CONFIDENCIALIDAD EN DIVULGACIONES PÚBLICAS

Los mecanismos de divulgación pública deben dar prioridad al mantenimiento de la confidencialidad de las personas informantes, a menos que se proporcione el consentimiento explícito. Las organizaciones deben establecer procesos claros y accesibles para que las personas informantes expresen sus preferencias con respecto a la divulgación y garantizar que se respeten estas preferencias.

5.12 EVALUACIÓN DE RIESGOS PREVIA A LA DIVULGACIÓN PÚBLICA

En el caso de las divulgaciones públicas, deben aplicarse marcos sólidos de evaluación de riesgos para evaluar las posibles consecuencias de la divulgación de información. Esto incluye evaluar la probabilidad de daño a las personas informantes, a las personas implicadas o al público. Cuando sea posible, deben aplicarse técnicas de anonimización y seudonimización a los datos antes de su divulgación.

5.13 USO DE HERRAMIENTAS DE REDACCIÓN AUTOMATIZADAS

El uso de soluciones tecnológicas, como las herramientas de redacción automatizadas, puede agilizar la preparación de los datos para su divulgación pública. Estas herramientas pueden detectar y enmascarar información personal confidencial de manera consistente y eficiente, minimizando el riesgo de error humano.

5.14 CRITERIOS CLAROS PARA LA DIVULGACIÓN PÚBLICA

Las organizaciones también deben establecer criterios claros para determinar cuándo es apropiada la divulgación pública. Los factores a tener en cuenta incluyen la urgencia del problema, la disponibilidad de mecanismos de presentación de denuncias internas o externas y los posibles beneficios y riesgos de la divulgación.

5.15 FORMACIÓN DEL PERSONAL EN PROCESOS DE DIVULGACIÓN PÚBLICA

Por último, son esenciales los programas de educación y formación para el personal que participa en los procesos de divulgación pública. Estos programas deben abarcar los aspectos legales y éticos de la protección de datos, la importancia de equilibrar la privacidad con la transparencia y las habilidades técnicas necesarias para manejar información confidencial.



Protección y apoyo a las personas informantes



Capítulo 4

PROTECCIÓN Y APOYO A LAS PERSONAS INFORMANTES

Capítulo 4

4.1 PROTECCIÓN PREVISTA EN LA DIRECTIVA 2019/1937/UE

La Directiva proporciona una protección integral a las personas que denuncian infracciones del Derecho de la Unión, garantizando que un amplio espectro de personas implicadas en actividades relacionadas con el trabajo estén protegidas contra las represalias. Esta protección se extiende más allá de los empleados tradicionales y abarca una amplia gama de personas:

- A. Los funcionarios, así como los trabajadores por cuenta propia, como los trabajadores por cuenta propia y los contratistas independientes (en virtud del artículo 49 del TFUE).
- B. Accionistas y consejeros no ejecutivos.
- C. Voluntarios y aprendices, remunerados o no.
- D. Extrabajadores.
- E. Facilitadores: personas físicas que asisten a las personas informantes de manera confidencial. Esto incluye asesores legales que ofrecen orientación estratégica, representantes sindicales que abogan por las personas informantes y otros intermediarios de confianza que ayudan a navegar por las complejidades de la divulgación.
- F. Terceros que podrían sufrir represalias debido a su conexión con la persona denunciante, incluidos familiares, colegas e incluso personas jurídicas vinculadas a la persona denunciante.

En particular, la protección de las personas informantes **no se aplica** a las personas que divulgan información directamente a la prensa, excepto en los casos en que las leyes nacionales establezcan protecciones específicas para la libertad de expresión e información (artículo 15.2). Como resultado, **los periodistas están excluidos de las protecciones de la Directiva**.

En **Bulgaria** se están haciendo intentos de incorporar aspectos del concepto SLAPP y de la legislación de protección de las personas informantes en la defensa de los casos contra periodistas. Sin embargo, sería útil contar con **pruebas** claras a nivel legislativo (legislación nacional y de la UE) y en la práctica, de que "la protección de la libertad de expresión en los casos de demandas estratégicas contra la participación pública (SLAPP) debe ir de la mano con la protección de las personas informantes". Sobre la base de esta consideración, la protección **sigue siendo válida independientemente** del canal elegido, siempre que la divulgación cumpla con las disposiciones de la Directiva. Si **los mecanismos internos o externos** resultan ineficaces o si existe una amenaza inminente para el interés público, las personas informantes pueden hacer públicas sus preocupaciones sin perder su **base legal** de protección.

Sin embargo, los diferentes grupos de interés **perciben los canales internos** como **menos seguros que los externos**, especialmente cuando las denuncias entran en conflicto con los intereses de una organización. Muchos temen represalias. Esta preocupación **se extiende al personal encargado de recibir y tramitar** las denuncias, que -al menos en **Italia**- a menudo carece de independencia de sus organizaciones y no goza de las salvaguardias necesarias que les permitan tramitar las denuncias de manera eficaz.

4.1.2 ¿QUÉ TIENE QUE HACER LAS PERSONAS INFORMANTES PARA TENER DERECHO A LA PROTECCIÓN?

Como se ha previsto, para poder acogerse a la protección en virtud de la Directiva, **las personas informantes deben cumplir determinadas condiciones**, a saber, que las denuncias se realicen a través de los canales adecuados y que las personas informantes tengan una **creencia razonable** de que la información revelada es verdadera. La **Directiva** no permite evaluaciones subjetivas de los motivos de un denunciante para denunciar una infracción. Por lo tanto, la "**buena fe**" no es un factor relevante, sino que lo que importa es que la persona informante **crea razonablemente** que se ha cometido o es probable que se cometa un delito. Este concepto, denominado razonabilidad, sustituye al estándar tradicional de buena fe.

¿Qué constituye una "creencia razonable"?

- A. Una **creencia razonable** se basa en elementos objetivos y concretos, como pruebas o indicaciones verificables, que llevan a la persona denunciante a creer que los hechos presentados son ciertos. Esto significa que, incluso si la información reportada posteriormente resulta ser incorrecta, el/la denunciante permanece protegido siempre que tenga motivos legítimos para considerarla precisa en el momento de la denuncia. Esta salvaguarda es crucial para alentar a las personas a dar un paso al frente sin temor a ser castigadas por errores involuntarios.
- B. El motivo personal **de un denunciante** para denunciar es **irrelevante** para su protección. Este principio se reafirma en el **considerando 32 de la Directiva** y se reitera en el apartado 14 de la Resolución 10/8 de la CNUCC "Protección de las personas informantes". A partir de 2019 se ha pasado **definitivamente de evaluar los motivos personales de la persona informante a evaluar los hechos objetivos de la propia denuncia**. El principio de razonabilidad también desempeña un papel crucial en la prevención de denuncias malintencionadas (es decir, afirmaciones manifiestamente falsas) que podrían perjudicar injustamente a personas u organizaciones. Sin embargo, el Convenio Europeo de Derechos Humanos (CEDH) sigue incluyendo la buena fe como requisito de protección, lo que crea un claro conflicto con la Directiva.

Lo que importa es que las denuncias se realicen en interés público o en interés de la integridad de la administración pública o de la entidad privada: las razones que llevaron a la persona a denunciar, denunciar o divulgar públicamente son irrelevantes a los efectos de su protección.

Protección en denuncias anónimas

Para garantizar la protección, las personas informantes deben utilizar los canales de denuncia descritos en el **Capítulo 2**.

CP. 2 >

La Directiva reconoce que las denuncias anónimas pueden ayudar a generar confianza en los sistemas de denuncia de irregularidades. Las personas informantes que optan por denunciar de forma anónima y luego revelan su identidad siguen teniendo derecho a la protección si se enfrentan a represalias (art. 6.3). Sin embargo, el tratamiento de la denuncia anónima varía en los tres países participantes en este proyecto y, en general, en toda Europa.

La legislación italiana no prevé la denuncia anónima, excepto el reconocimiento de la protección a las personas informantes anónimos que sufren represalias. ANAC, que gestiona el **canal externo**, trata las denuncias anónimas como quejas ordinarias hasta que se invoca la protección. Si una persona denunciante anónimo se enfrenta posteriormente a represalias, tiene derecho a las mismas protecciones que las personas informantes no anónimos (**artículo 6 del Decreto Legislativo 24/2023**). Una diferencia clave con respecto a la denuncia anónima es que el acceso a la denuncia se considera permitido bajo condiciones y limitaciones específicas establecidas por la ley italiana. Esto se debe a que las denuncias anónimas se tratan como denuncias ordinarias en virtud de las disposiciones legales generales: a) acceso documental y defensivo (artículos 22 y siguientes de la Ley n.º 241/1990), y b) acceso cívico (artículos 5 y siguientes del Decreto Legislativo n.º 33 de 2013).

Bulgaria no regula formalmente la denuncia anónima. Sin embargo, las personas que han presentado denuncias anónimas o divulgado públicamente información sobre violaciones, y que posteriormente son **identificadas y sometidas a represalias, tienen derecho a protección (artículo 10 de la Ley búlgara de denuncia de irregularidades).**

España permite la denuncia anónima y obliga a proteger a **las personas informantes que posteriormente sean identificados y objeto de represalias (artículo 7.3 para la denuncia interna y artículo 17 para la denuncia externa, Ley 2/2023, de 20 de febrero).** Según la legislación española, la vulneración de las garantías de confidencialidad y anonimato constituye una infracción muy grave dentro del régimen sancionador. Se prohíbe cualquier acción u omisión destinada a revelar la identidad de un informante que haya optado por el anonimato, incluso si la divulgación real no se produce.

4.2 MEDIDAS DE APOYO DE LAS ENTIDADES OBLIGADAS

La primera medida de apoyo (artículo 20 de la Directiva) es ofrecer información y asesoramiento completos e independientes, de fácil acceso al público y gratuitos. Esto incluye orientación sobre: a) los procedimientos y recursos disponibles, b) la protección contra las represalias, y c) los derechos de la persona interesada. Además, las personas informantes deben recibir

asistencia efectiva de las autoridades competentes ante cualquier autoridad pertinente involucrada en su protección contra represalias. Esto incluye:

- A. Certificación, cuando así lo prevea la legislación nacional, que confirme que reúnen los requisitos para la protección.
- B. Asistencia jurídica gratuita en procesos penales y civiles transfronterizos, de conformidad con la Directiva y la Directiva 2008/52/CE del Parlamento Europeo y del Consejo (48).
- C. Cuando lo permita la legislación nacional, asistencia jurídica adicional, asesoramiento jurídico u otro tipo de asistencia jurídica en procedimientos posteriores.

4.2.1 EL PAPEL DE LAS AUTORIDADES

- A. Las **autoridades competentes** deben apoyar activamente a **las personas informantes** que sufran represalias, sirviendo como su primer punto de contacto.
- B. Las personas informantes deben informar de su situación a estas autoridades, que son **responsables de hacer cumplir la Directiva** en su Estado miembro.
- C. Las autoridades evalúan si la persona **cumple con los criterios de protección** y si ha enfrentado medidas de represalia.
- D. Las autoridades deben garantizar que las personas informantes reciben el reconocimiento y la asistencia jurídicos adecuados.

4.2.2 FORMAS DE APOYO PREVISTAS EN LA DIRECTIVA 2019/1937/UE

El considerando 90 de la Directiva establece que **las autoridades competentes** deben proporcionar a las personas informantes el **apoyo necesario** para acceder eficazmente a la protección. En particular, deberían: a) proporcionar **pruebas u otra documentación** que confirme a otras autoridades o tribunales que se **ha realizado una denuncia externa**, y b) asegurarse de que las personas informantes comprendan **sus derechos y los recursos disponibles**.

Buscar **orientación profesional** puede proporcionar la confianza necesaria para navegar por el proceso y, al mismo tiempo, garantizar el más alto nivel de protección según la ley.

Acciones legales contra las represalias

Debe haber asistencia legal gratuita **e independiente** para ayudar a las personas informantes a navegar por los procesos de denuncia y comprender sus derechos. Algunas jurisdicciones extienden la asistencia jurídica tanto a **los procedimientos civiles como a los penales** relacionados con casos de protección de las personas informantes. Si un/a denunciante **se enfrenta a represalias**, como el despido, la degradación o el acoso, tiene derecho a **solicitar recursos legales**, incluidas medidas provisionales y una indemnización completa (art. 21.8).

Para respaldar su afirmación, las personas informantes **deben proporcionar pruebas** que demuestren que hicieron una denuncia y que se tomaron

medidas de represalia contra ellos. **Los juzgados y tribunales nacionales** desempeñan un papel crucial en **la aplicación de estas protecciones, garantizando que las personas afectadas vuelvan** a su situación anterior y sean indemnizadas por los daños sufridos.

En los procedimientos judiciales⁵⁷ relativos a los daños sufridos por un/a informante, si el denunciante demuestra que ha denunciado una infracción y ha sufrido un daño, se presume que el daño fue consecuencia de represalias. En tales casos, la carga de la prueba se traslada a la parte que adoptó la medida desfavorable, que debe demostrar que la acción se basó en motivos debidamente justificados.

Un ejemplo práctico en España: se creó un fondo de apoyo jurídico, social y psicológico gratuito para las personas informantes. Los **Países Bajos** han puesto en marcha una iniciativa similar. En **Francia**, las personas informantes pueden recibir provisiones para las costas judiciales y subvenciones en los recursos contra las medidas de represalia o en la defensa contra acciones legales destinadas a obstaculizar su denuncia o divulgación pública.

Es interesante notar que, en **Italia**, en casos de intento o amenaza de represalia, la ley de implementación establece que la persona informante debe presentar elementos que demuestren la probabilidad ("*fumus*") de la amenaza o intento de represalia. La carga de la prueba se traslada entonces a la parte acusada de represalias, exigiéndole que demuestre que los presuntos actos no están relacionados con el informe de la informante. Se trata de la inversa de la carga de la prueba prevista por la Directiva como imperativa. En **Italia** está previsto por la ley de aplicación, no exigido por la ANAC.

Además de la asistencia legal, las personas informantes **pueden recibir apoyo psicológico y financiero**, especialmente cuando las represalias causan angustia emocional y/o dificultades económicas. En algunos casos, las autoridades pueden reconocer formalmente la condición de un/a denunciante, reforzando su protección legal y credibilidad.

Acceso a los servicios de soporte

Para proteger aún más a las personas informantes, los Estados miembros deben establecer servicios de asesoramiento independientes que proporcionen asistencia jurídica, orientación práctica, información y apoyo. Las personas informantes pueden recurrir a estos servicios para obtener asesoramiento confidencial sobre sus derechos, los recursos disponibles y las opciones legales. Estas estructuras de apoyo están diseñadas para empoderar a las personas, garantizando que puedan navegar por el proceso de denuncia y protección con confianza. De acuerdo con la Directiva, estos servicios pueden ser prestados por una institución pública o por entidades cívicas.

La legislación española permite explícitamente la asistencia efectiva de cualquier autoridad pertinente implicada en la protección de las personas informantes frente a represalias, incluida la emisión de una certificación que confirme su elegibilidad para la protección de la ley.

⁵⁷ Art. 38.4 Ley 2/23 española, búlgara... art. 19 de la ley italiana 24/2023

Represalias más allá del lugar de trabajo

Las represalias contra las personas informantes van más allá de las consecuencias laborales, como el despido o la degradación. También puede incluir:

- A. Hostigamiento e intimidación.
- B. Daño reputacional.
- C. Campañas de desprestigio en las redes sociales.
- D. Listas negras de la industria, que pueden afectar gravemente las perspectivas profesionales de un informante.

La Directiva aborda explícitamente estos riesgos, garantizando la protección más allá del lugar de trabajo y reconociendo que las personas informantes pueden enfrentarse a consecuencias sociales más amplias.

La legislación italiana garantiza explícitamente una protección que abarca también las represalias que pueden consistir en daños económicos o financieros, incluida la pérdida de oportunidades económicas y la pérdida de ingresos; terminación anticipada o cancelación del contrato de suministro de bienes o servicios; cancelación de una licencia o permiso; Solicitud injustificada de exámenes psiquiátricos o médicos.

Certificación por parte de las autoridades competentes

En algunos Estados miembros, la condición formal de informante es un requisito previo para recibir apoyo y medidas de protección. En algunos Estados miembros, la condición de informante se reconoce mediante la presentación de una "certificación de informante", tal como se indica en el considerando 90, apartado 1, de la Directiva. Entre los países que han introducido esta certificación se encuentran **Francia, Letonia, Polonia** y **España**, concretamente en el caso de la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana (AVAF). Esta certificación sirve como reconocimiento formal de su estatus y puede ser útil en procedimientos legales o cuando se busca asistencia de instituciones públicas o privadas. Fortalece su caso cuando necesitan demostrar su derecho a las medidas de protección.

En virtud **de determinados marcos nacionales, las personas informantes pueden optar a la certificación**, lo que confirma que cumplen los requisitos legales de protección. Sin embargo, incluso en ausencia de certificación, las personas informantes deben tener acceso efectivo a la **revisión judicial**. Los tribunales decidirán en última instancia, sobre la base de todas las circunstancias individuales del caso, si un/a informante califica para la protección bajo las reglas aplicables.

4.3 AMPLIACIÓN DEL ALCANCE DE LAS INFRACCIONES

Si bien la Directiva se centra principalmente en las violaciones de la legislación de la UE, anima a los Estados miembros a ampliar la protección a las infracciones de la legislación nacional y a las conductas poco éticas que, aunque no sean ilegales, plantean riesgos para la sociedad. Al ampliar el alcance de las divulgaciones protegidas, los Estados miembros pueden reforzar las salvaguardias de las personas informantes, garantizando una mayor protección contra las conductas indebidas que puedan perjudicar el interés público, la democracia o la integridad institucional.

PERSPECTIVA DE GÉNERO

Proteger a las personas informantes requiere un **enfoque inclusivo**, reconociendo que las personas de **grupos marginados** o aquellas que enfrentan vulnerabilidades interseccionales pueden experimentar **un mayor riesgo de represalias** y un mayor miedo que otras. El riesgo de represalias **puede influir en** si una persona decide denunciar y cómo. Las investigaciones, incluidos los estudios realizados por Transparencia Internacional, confirman que las mujeres pueden experimentar un mayor miedo y estrés al denunciar conductas indebidas (véase el recuadro de perspectiva de género en el [capítulo 5](#)).

CP. 5 ➤

Uno de los principales factores que influyen en la decisión de las mujeres de denunciar conductas indebidas es la dinámica de poder en el lugar de trabajo:

- A. Desequilibrios de poder dentro de la organización: Los entornos de trabajo suelen estar dominados por hombres en puestos de poder y autoridad en la toma de decisiones. Cuanto mayor sea el **desequilibrio** de poder entre hombres y mujeres, mayor será el riesgo de represalias para las personas informantes.
- B. Las represalias contra las mujeres a menudo se dirigen a su esfera personal: a diferencia de otras formas de represalia, las mujeres pueden experimentar **ataques íntimos y personales**, como comentarios sexistas o acoso por motivos de género.
 - I. **Bulgaria:** Las organizaciones de la sociedad civil han expresado su preocupación por el creciente número de acciones legales contra las personas informantes de irregularidades en el periodismo. A menudo se percibe a las mujeres periodistas como el sexo débil, lo que las convierte en blancos más fáciles para las tácticas de intimidación y miedo.
- C. Impacto psicológico y de salud: Las investigaciones muestran que las mujeres se toman la **licencia por enfermedad** con más frecuencia que los hombres después de denunciar conductas indebidas, a menudo como una forma de evitar represalias en el lugar de trabajo.
 - I. **Italia:** Los estudios han puesto de manifiesto que las desventajas a las que se enfrentan las mujeres en la denuncia de irregularidades también se manifiestan como **una menor conciencia** de sus derechos y una menor capacidad para protegerse en los procedimientos judiciales.

Para hacer frente a estos desafíos basados en el género, las organizaciones deben:

- A. **Elaborar y aprobar protocolos que tengan en cuenta las cuestiones de género** (véase el recuadro del [capítulo 1](#)):
 - I. Con consenso y una representación adecuada, las organizaciones deben establecer protocolos o directrices específicos para gestionar los casos de denuncia de irregularidades relacionadas con el género.
 - II. Garantizar que estos protocolos se integren tanto en las políticas de protección de informantes como en las políticas de igualdad y no discriminación de la organización.
 - III. Estos protocolos deben describir procedimientos claros para denunciar, investigar y abordar los casos de violencia de género, acoso o discriminación.
 - IV. Todas las personas deben estar plenamente informadas de sus derechos y de los servicios de apoyo disponibles.

CP. 1 ➤

Ampliar el acceso a la asistencia jurídica, al apoyo psicológico y a los servicios externos.

- I** Garantizar que las mujeres y otros grupos expuestos a la discriminación dispongan de asistencia jurídica, para que puedan defenderse mejor de las represalias y las acciones legales.
- II** Garantizar que los mecanismos de denuncia estén diseñados para evitar represalias y revictimización en los casos de género, asegurándose de que las personas dentro de la misma jerarquía en el lugar de trabajo, como supervisores o colegas, no puedan acceder a las denuncias. Las personas informantes deben sentirse seguros de que su identidad y sus acciones estarán protegidas, especialmente en casos delicados de género en los que el riesgo de represalias es mayor.
- III** Proporcionar información sobre servicios de apoyo externo, incluida la asistencia jurídica, el apoyo psicológico y las organizaciones de defensa de los supervivientes. Esto permite que los posibles informantes se sientan más seguros e informados a la hora de considerar si denunciar una mala conducta y de enfrentarse a cualquier desafío que puedan enfrentar durante el proceso.

CP. 1 ➤

En concreto, en **España** el ámbito material **de protección se aplica a las personas físicas que denuncien tanto acciones u omisiones previstas en el ámbito material** de aplicación de la Directiva, como acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave en el ordenamiento jurídico español, y "en todo caso, todas aquellas infracciones penales o administrativas graves o muy graves que impliquen un perjuicio económico para la Hacienda Pública y para el Bien Social" Se entenderá incluida la garantía" (Art. 2.1.b) Ley 2/23).

4.4 DIVULGACIÓN PÚBLICA Y SITUACIONES DE EMERGENCIA

Por lo general, se anima a las personas informantes a denunciar interna o externamente antes de hacer pública su divulgación. Sin embargo, permanecen protegidos si la divulgación pública (de conformidad con el artículo 15 de la Directiva) es necesaria debido a amenazas inminentes, como desastres ambientales, riesgos para la salud o fraude financiero, o si las pruebas pueden destruirse o las autoridades se ven comprometidas⁵⁸. (detallar mejor: En **España**, las personas informantes deben cumplir requisitos **específicos** para obtener protección al hacer una **divulgación pública**. Estos requisitos deben detallarse, en lugar de basarse en información genérica. *(Considere agregar los criterios legales específicos requeridos en **España** para que las divulgaciones públicas estén protegidas)*. En **Italia** también.

4.5 PÉRDIDA DE PROTECCIÓN

La protección puede ser revocada bajo condiciones específicas para evitar el uso indebido mientras se mantiene la integridad del sistema:

⁵⁸ De acuerdo con la legislación española, la persona que haga una divulgación pública tendrá derecho a la protección de la Ley "si se cumplen las condiciones de protección reguladas en el Título VII y alguna de las siguientes condiciones:

- a. Que hayan realizado la comunicación previamente por canales internos y externos, o directamente por canales externos, de conformidad con los títulos II y III, sin que se hayan tomado las medidas adecuadas al respecto en el plazo establecido.
- b. Que tiene motivos razonables para creer que la violación puede constituir un peligro inminente o manifiesto para el interés público, en particular cuando se trata de una situación de emergencia, o existe un riesgo de daño irreversible, incluido un peligro para la integridad física de una persona; o, en caso de comunicación a través de un canal de información externo, existe el riesgo de represalias o hay pocas probabilidades de que la información se trate de manera efectiva debido a las circunstancias particulares del caso, como el ocultamiento o la destrucción de pruebas, la colusión de una autoridad con el autor de la infracción, o que la autoridad esté involucrada en la infracción.

2. Las condiciones de protección previstas en el párrafo anterior no se aplicarán cuando la persona haya divulgado información directamente a la prensa en conformidad con el ejercicio de la libertad de expresión y veraz prevista en la Constitución y su legislación reglamentaria." (Art. 28, Ley 2/23).

- A. **Denuncias maliciosas:** Las personas informantes que, a sabiendas, proporcionan información falsa o engañosa pierden su protección. Los Estados miembros podrán imponer sanciones en tales casos.
- B. **Incumplimiento de los procedimientos:** La denuncia fuera de los canales designados suele dar lugar a la pérdida de la protección, excepto en casos de amenazas urgentes o destrucción de pruebas.
- C. **Actividades ilegales:** Las personas informantes que participan en la piratería, el robo de datos o el acceso no autorizado no están protegidos para garantizar un uso responsable del sistema.
- D. **Violación de la confidencialidad:** Si la persona informante divulga información excesiva o sensible sin justificación, la protección puede ser revocada.
- E. **Divulgación pública inadecuada:** Las personas informantes deben intentar primero informar de forma interna o externa, a menos que exista una justificación válida para la exposición pública urgente.

4.6 Apoyo a las personas informantes: ¿Quién puede ayudar?

La Directiva (considerando 41 y posteriormente art. 4) amplía la protección a quienes asisten a las personas informantes, garantizando que todos los implicados puedan operar de forma segura y eficaz.

Facilitadores

Los facilitadores, como los asesores jurídicos y los representantes sindicales, ayudan a los denunciantes a denunciar las infracciones de forma segura. Su función incluye:

- A. Proporcionar orientación jurídica.
- B. Garantizar el cumplimiento de los procedimientos de presentación de denuncias.
- C. Mantener el anonimato de las personas informantes.

El artículo 2.1 de la ley italiana define al facilitador como "la persona que asiste a la persona informante en el proceso de denuncia, trabajando en el mismo contexto y cuya asistencia debe ser confidencial". La asistencia ofrecida por el facilitador podrá consistir en asesoramiento o apoyo a la persona informante. Por ejemplo, el facilitador podría ser un colega del denunciante que le asista de manera confidencial.

El artículo 5 de la ley búlgara estipula que también se concederá protección a "las personas que asistan a la persona informante en el proceso de denuncia y cuya asistencia sea confidencial". La ley no se refiere a estas personas como "facilitadores" y no proporciona ningún detalle sobre en qué puede consistir esta asistencia.

La legislación española reconoce expresamente a los facilitadores como sujetos protegidos. Según el **artículo 3.3** de la Ley: También estarán amparadas por esta Ley las personas físicas que asistan al informante en el proceso, incluidas las que le presten apoyo en el ámbito laboral, y aquellas que estén relacionadas con él y puedan sufrir represalias en un contexto laboral o profesional, así como las personas jurídicas propiedad del informante, para las que trabaje o con las que mantenga una relación en un

contexto laboral o en las que ostente una participación significativa. En este sentido se incluye a facilitadores como: Asesores jurídicos, Representantes sindicales, Compañeros de trabajo y Personas que prestan apoyo psicológico o institucional.

Su protección tiene por objeto evitar represalias indirectas y garantizar que el informante pueda actuar con seguridad, especialmente en entornos laborales sensibles. Esta ampliación del ámbito subjetivo de protección responde a lo previsto en el considerando 41 y el artículo 4 de la Directiva, asegurando que todas las personas que intervienen de buena fe en el proceso de denuncia puedan operar sin temor a consecuencias negativas.

Organizaciones de terceros

Las ONG y los grupos de la sociedad civil pueden:

- A. Ofrecer apoyo a los y las posibles informantes que actúen como centros de información (véase más abajo), proporcionando asesoramiento práctico sobre la denuncia y los derechos legales, asistencia para la denuncia, apoyo psicológico para ayudar a las personas informantes a gestionar el estrés y la reacción social.
- B. Ofrecer canales seguros y visibilidad para la divulgación pública, facilitando el acceso a los medios de comunicación o permitiendo la publicación a través de plataformas independientes.

Autoridades competentes

Autoridades designadas por el Estado:

- A. Orientar a las personas informantes sobre los procedimientos de denuncia.
- B. Explique los mecanismos de protección.
- C. Certificar la condición de informante, cuando corresponda, para evitar represalias.

Centros de Información

Los organismos administrativos independientes sirven como centros centralizados para el apoyo a las personas informantes, ofreciendo asesoramiento legal, asesoramiento y coordinación de los recursos disponibles. También las organizaciones de la sociedad civil pueden desempeñar este papel. En **Italia**, la ley asigna un papel crucial a las organizaciones del Tercer Sector en el apoyo a las personas informantes. Las organizaciones proporcionan información, asistencia y asesoramiento gratuitos sobre cómo denunciar y sobre la protección frente a represalias que ofrece la legislación nacional y de la UE, sobre los derechos de la persona afectada y sobre las condiciones de acceso a la asistencia jurídica gratuita.

Colegas y supervisores de apoyo

Los colegas o supervisores de confianza pueden:

- A. Brindar apoyo informal.
- B. Ayudar a refinar las denuncias para garantizar la precisión.
- C. Facilitar el uso correcto de los canales internos de denuncia.

Proveedores de Asistencia Legal

Las organizaciones de asistencia jurídica, tanto públicas como privadas, asisten a las personas informantes que se enfrentan a represalias, apoyándoles en los procedimientos judiciales para buscar reparación o defender sus derechos.

Apoyo psicológico y social

La Directiva (art. 89 y art. 20) establece que se anima a los Estados miembros a proporcionar servicios de asesoramiento y apoyo social adaptados para ayudar a las personas a hacer frente a los retos emocionales y sociales a los que puedan enfrentarse. Esto forma parte de las medidas de protección e incluye ofrecer acceso a asesoramiento psicológico, así como a servicios de asesoramiento legal y financiero para mitigar las posibles repercusiones profesionales y económicas. Además, las redes de apoyo, como los grupos de pares o los programas de tutoría, pueden ayudar a las personas informantes a sortear la reacción social y reducir los sentimientos de aislamiento. Las campañas de concienciación pública también pueden desempeñar un papel en el fomento de una cultura que valore la denuncia de irregularidades, la reducción del estigma y el fomento de la solidaridad dentro de las comunidades y los lugares de trabajo. Al aplicar estas medidas, los Estados miembros pueden crear un entorno más propicio que no solo proteja a las personas informantes, sino que también les permita actuar en aras del interés público sin temor a represalias.

Apoyo financiero

Solo algunos países ofrecen medidas de apoyo económico en su marco jurídico, pero su alcance y su cuantía son limitados. Entre ellos, Bélgica y Eslovaquia cubren los costes de la asistencia jurídica privada y los costes de los gastos sanitarios y/o psicológicos privados.

Protecciones para los asistentes

La Directiva también protege a quienes asisten a los denunciantes, en particular:

- A. Facilitadores.
- B. Familiares.
- C. Colegas.

Esto garantiza que puedan ayudar a las personas informantes sin temor a represalias.

Libertad de prensa y acceso a la información

La libertad de prensa desempeña un papel fundamental a la hora de garantizar que las personas informantes puedan compartir sus revelaciones de forma segura. Los gobiernos deben proteger la independencia de los medios de comunicación, salvaguardar a los periodistas que cubren los casos de denuncias y mantener la confidencialidad de las fuentes. Además, el acceso a la información es crucial: las personas informantes necesitan marcos legales transparentes que les permitan fundamentar sus afirmaciones con pruebas.

PERSPECTIVA DE GOBIERNO ABIERTO

Protección de las personas informantes

Una protección eficaz de los denunciantes se beneficiaría de esfuerzos coordinados entre diversos actores, como instituciones, organizaciones de medios de comunicación, grupos de la sociedad civil, sindicatos y organismos de derechos humanos. Este enfoque colaborativo reconoce el papel crucial de los denunciantes en todos los sectores y refuerza la narrativa que vincula su denuncia y protección con los derechos laborales y la libertad de expresión. Esta conexión es particularmente relevante en los países que experimentan un aumento de las demandas estratégicas contra la participación pública (SLAPP).

Los profesionales de todos los sectores han indicado que cuando la Directiva se implementa a través de la creación de nuevas autoridades u oficinas dedicadas a la denuncia de irregularidades, la **participación de múltiples partes interesadas puede ser decisiva para generar confianza entre todas las partes involucradas**, especialmente si se lleva a cabo en el marco de la implementación de OGP en el país. Procesos como los que se encuentran en la Alianza para el Gobierno Abierto (OGP, por sus siglas en inglés) ofrecen una plataforma útil para ese diálogo entre múltiples partes interesadas. En particular, esto puede ayudar a profundizar aún más la participación de los representantes del sector privado, ya sea como entidades individuales o a través de órganos representativos, y contribuir así a un debate más equilibrado y a mecanismos de protección más eficaces.

La participación significativa de las partes interesadas también debe **extenderse a la participación en foros internacionales como la Convención de las Naciones Unidas contra la Corrupción (CNUCC)**. Esto incluye garantizar que los y las informantes, así como las organizaciones dedicadas a su protección, participen activamente en las delegaciones nacionales y en los debates preparatorios. Un claro ejemplo de este enfoque se vio en la CoSP10 de la CNUCC en Atlanta⁵⁹, donde la resolución sobre la protección de las personas informantes fue encabezada por un/a ex denunciante que fue incluido directamente en la delegación serbia. Esto demuestra el valor de incorporar la primera experiencia en la formulación de políticas, asegurando que aquellos que han enfrentado represalias o han navegado por el proceso de presentación de denuncias contribuyan a dar forma a protecciones más efectivas. **Al integrar a las personas informantes y a los grupos de defensa en las delegaciones oficiales, los grupos de trabajo y los procesos de negociación**, los países pueden desarrollar políticas que no solo estén bien informadas, sino que también sean prácticas y aplicables. Este enfoque inclusivo mejora la legitimidad, fortalece la cooperación internacional y garantiza que los marcos de protección de las personas informantes se basen en los desafíos y necesidades del mundo real.

⁵⁹ Ver: <https://whistleblowingnetwork.org/News-Events/News/News-Archive/Governments-Around-the-World-Step-Up-to-Support-Wh>

Además de estas medidas de colaboración, las OSC recomiendan encarecidamente una **interpretación amplia** de las leyes de protección de las personas informantes, que vaya más allá de las disposiciones de la Directiva y allane el camino para su futura reforma.

- A. Una propuesta clave es ampliar las salvaguardias a las **organizaciones que brindan apoyo y asesoramiento a las personas informantes**, garantizando que quienes ayudan a las personas informantes también estén protegidos de amenazas y represalias. Los gobiernos y la sociedad civil pueden colaborar en esta expansión, reconociendo el papel crucial que desempeñan estas organizaciones para permitir divulgaciones seguras y efectivas.
- B. Otro paso crucial es lograr **una mayor armonización** entre los mecanismos de protección de las personas informantes y otros marcos jurídicos, como los diseñados para los **programas de protección de testigos y la denuncia en relación con la corrupción en la que participan grupos delictivos organizados**. Un enfoque más integrado ayudaría a garantizar que las personas que denuncien irregularidades reciban medidas de seguridad adecuadas.
- C. A pesar de no estar explícitamente contempladas en la Directiva, las OSC abogan por ampliar la protección a los casos en los que se exponga la mala conducta o la corrupción **a través del acceso a la información pública**. Esto incluye las revelaciones hechas por **periodistas, ONG, defensores legales y ciudadanos activos** que, en aras del interés público, descubren y denuncian irregularidades.

Varios instrumentos internacionales respaldan esta interpretación más amplia de la protección las personas informantes. La propia Directiva 2019/1937/UE sobre informantes de irregularidades, la Ley Europea de Libertad de los Medios de Comunicación (EMFA) y la Convención de las Naciones Unidas contra la Corrupción (CNUCC) con sus resoluciones conexas, contribuyen a crear un entorno jurídico más favorable para ampliar y armonizar las salvaguardias. Al fortalecer las protecciones legales y ampliar su alcance, los gobiernos pueden mejorar la transparencia, fomentar la rendición de cuentas y crear condiciones más seguras para quienes se pronuncian en contra de las irregularidades tanto en el sector público como en el privado.

Apoyo a las personas informantes

Una iniciativa positiva de gobierno abierto en apoyo a los y las posibles informantes es establecer un **registro público de OSC que brindan servicios gratuitos de apoyo y asesoramiento**, para mejorar su reconocimiento y visibilidad. En el caso de **Italia**, este objetivo se logró al incluir el compromiso en su 5º Plan de Acción Nacional (5NAP) para el Gobierno Abierto (2021-2023).⁶⁰ Para aquellos que deseen replicar la iniciativa italiana, recomendamos:

- A. Definir los requisitos para que las OSC ingresen a la lista pública, a fin de garantizar la imparcialidad, el respeto de las normas de privacidad y la competencia.
- B. Fomentar la experiencia profesional diversa dentro de las OSC para garantizar un apoyo integral (legal, psicológico, etc.).
- C. Establecer un convenio formal con la autoridad para las OSC adecuadas.
- D. Mantener un grupo de trabajo activo entre los miembros del registro para supervisar las necesidades de capacitación e información y facilitar el intercambio entre pares.
- E. Establecer al menos dos veces al año foros para abordar los desafíos sistémicos que enfrentan las OSC y las preocupaciones que surgen de casos reales, respetando al mismo tiempo la protección de la confidencialidad.
- F. Alentar o exigir a todos los organismos públicos que sigan el ejemplo de la autoridad en la visibilidad de la lista también en su sitio web y en la comunicación a sus empleados.

Otra medida avanzada en el marco del gobierno abierto es establecer la coordinación y el trabajo en red entre entidades asesoras y de apoyo reconocidas para garantizar que potenciales informantes sean dirigidos a la organización más adecuada para recibir orientación. Por ejemplo, **podría crearse un centro centralizado** para recopilar y evaluar las necesidades de las personas informantes y derivarlos a la organización de apoyo adecuada en función de la experiencia territorial o sectorial. Esto ayudaría a agilizar el proceso y garantizaría que las personas reciban la asistencia más eficaz.

⁶⁰ Ver: <https://www.opengovpartnership.org/members/italy/>

Estos servicios de apoyo jurídico y psicológico deben ser gratuitos para los/las posibles denunciantes, a fin de eliminar cualquier barrera económica que impida el acceso a los servicios. Para garantizar esto, el gobierno debería asegurar financiación **pública para apoyar a las organizaciones** (institucionales y cívicas) y **asistencia legal gratuita** para las personas informantes en lo que respecta a los juicios.

4.7 RECOMENDACIONES

Para ofrecer apoyo y protección integrales a las personas que acceden a los procedimientos de denuncia, es de suma importancia fomentar un enfoque eficaz y colaborativo de la denuncia de irregularidades. Esto requiere la participación de múltiples partes interesadas, cada una de las cuales aporta su experiencia y su papel para abordar los desafíos asociados con la denuncia de irregularidades. Las medidas clave para mejorar el apoyo y la protección de las personas informantes incluyen:

1. MEJORAR LA ACCESIBILIDAD A APOYO PARA PERSONAS INFORMANTES

Las entidades públicas y privadas deben mejorar la accesibilidad mediante la publicación de listas de organizaciones de la sociedad civil (OSC) y otros organismos pertinentes que ofrecen asistencia e información a las personas informantes.

2. FOMENTAR LA COOPERACIÓN ENTRE ACTORES CLAVE

La cooperación continua entre las autoridades competentes, las organizaciones de la sociedad civil y otras organizaciones pertinentes es crucial para garantizar que estén bien equipadas para prestar servicios de alta calidad a las personas informantes.

3. PROMOVER CONCIENCIACIÓN Y FORMACIÓN ESPECÍFICA

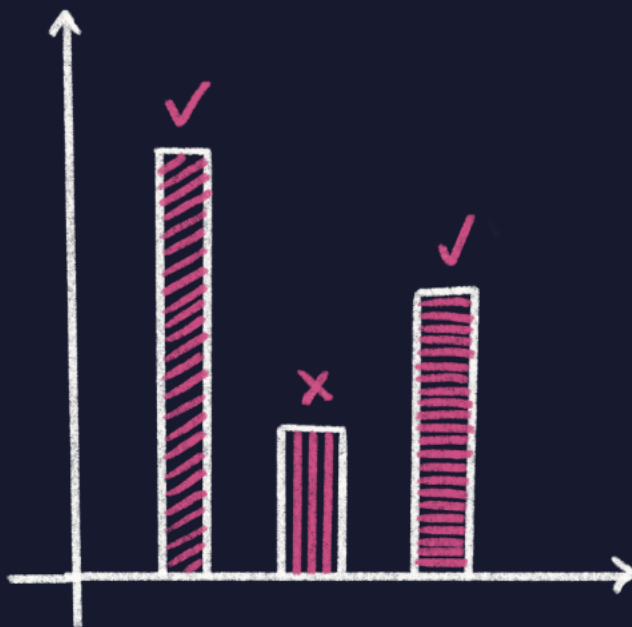
Las administraciones y las empresas deben promover activamente iniciativas de concienciación y programas de formación para mejorar la comprensión de las normas y procedimientos de denuncia de irregularidades. Además, se deben implementar cursos de capacitación específicos para funcionarios públicos a fin de desarrollar las mejores prácticas para el manejo de las denuncias de irregularidades y la gestión eficaz de los procesos relacionados.

4. ORGANIZAR ESPACIOS DE DIÁLOGO INTERSECTORIAL

Por último, la organización de reuniones específicas con representantes de los sectores público y privado puede facilitar un diálogo constructivo, lo que permite a las partes interesadas abordar desafíos comunes e identificar soluciones óptimas en colaboración.



Medición y evaluación de la eficacia del sistema y evaluación de la cultura de denuncia de irregularidades



Capítulo 5

MEDICIÓN Y EVALUACIÓN DE LA EFICACIA DEL SISTEMA Y EVALUACIÓN DE LA CULTURA DE DENUNCIA DE IRREGULARIDADES

Capítulo 5

5.1 MEDIR LO QUE IMPORTA: EFECTIVIDAD, CONCIENCIA Y AJUSTE CULTURAL

Contar con sistemas eficaces de denuncia de irregularidades contribuyen a **reforzar la transparencia** y la **rendición de cuentas** en la UE. Para garantizar su impacto, la eficacia de estos sistemas, junto con el nivel de concienciación y comprensión del proceso de denuncia de irregularidades, debe medirse y evaluarse periódicamente. Con la Directiva, a pesar de retos como el retraso en la transposición en la mayoría de los Estados miembros, la integración incompleta en los sistemas jurídicos nacionales y la aparente complejidad del marco, la atención se ha desplazado hacia la evaluación de la eficacia de estos sistemas y los factores culturales que influyen en su éxito.

En **Bulgaria** se ha puesto de manifiesto que existe cierta confusión y que los trabajadores a veces tienen dificultades para comprender el ámbito de aplicación de la Directiva, en particular cuando se trata de derechos laborales o violaciones que pueden parecer personales en lugar de afectar al interés público en general.

Un **encuestado italiano** reconoció que la nueva legislación sobre denuncia de irregularidades ha introducido innovaciones positivas, pero destacó una serie de cuestiones críticas, como un problema de coordinación en el caso de las divulgaciones a través de las redes sociales.

Según una respuesta de España, la aplicación de la ley debería haber ido acompañada de reformas procesales, incluido el fortalecimiento de las medidas de protección.

Los desarrollos recientes ponen de relieve la necesidad de evaluar los sistemas de denuncia de irregularidades no solo como herramientas de cumplimiento, sino como **mecanismos integrales** para promover el

comportamiento ético y la integridad organizacional. La investigación y la práctica contemporáneas ponen de manifiesto la necesidad de contar con métodos de evaluación exhaustivos para garantizar que los canales de denuncia de irregularidades sean accesibles, fiables y eficaces para hacer frente a las irregularidades, al tiempo que se protege a las personas informantes de las represalias. Además, la dimensión cultural, que abarca la confianza, la concienciación y la voluntad de los empleados de denunciar, se ha convertido en una piedra angular en la creación **de una cultura proactiva de denuncia**.

5.2 REVISIÓN DE LOS INSTRUMENTOS DE MEDICIÓN Y EVALUACIÓN EXISTENTES

5.2.1 ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN

El marco ISO 37002:2021 sirve como herramienta analítica para la formulación de políticas y ofrece información sobre la implementación de sistemas de gestión de denuncias (WMS) en diferentes instituciones.⁶¹ Proporciona directrices para establecer, implementar y mantener un Sistema de Gestión de Anticorrupción (SGA) eficaz basado en los principios de confianza, imparcialidad y protección. El marco describe cuatro pasos clave:

- A. Recibir denuncias de irregularidades,
- B. Evaluar las denuncias recibidas,
- C. Teniendo en cuenta las denuncias recibidas, y
- D. Cierre de casos de denuncia de irregularidades. Diseñadas para ser universalmente aplicables, estas directrices son relevantes para organizaciones de todos los tamaños, tipos y sectores, incluidas las entidades públicas, privadas y sin fines de lucro.

El marco proporciona un enfoque estandarizado para evaluar los sistemas de denuncia de irregularidades, con el objetivo de facilitar la formulación de políticas y las mejoras de la gobernanza. Los estudios de caso existentes ponen de manifiesto que la aplicación de esta norma para los sistemas de gestión de la denuncia de irregularidades suele ser parcial y requiere un mayor desarrollo en áreas específicas, como la concienciación de las personas informantes y las políticas de protección. En consecuencia, puede ser necesario adaptar el marco para satisfacer las necesidades específicas de la organización.

5.2.2 PLATAFORMAS DIGITALES DE DENUNCIA

La Ley de Servicios Digitales (DSA, por sus siglas en inglés)⁶² introduce herramientas para crear un espacio en línea más seguro, justo y

⁶¹ Organización Internacional de Normalización, ISO 37002:2021. Sistemas de gestión de denuncias de irregularidades: directrices, <https://www.iso.org/obp/ui/en/#iso:std:65035:en>

⁶² Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo al mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Ley de Servicios Digitales), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065>

transparente en la UE.⁶³ Entre ellas se encuentra la herramienta de denuncia de irregularidades de la DSA, que permite identificar prácticas nocivas de plataformas en línea muy grandes y motores de búsqueda en línea (VLOP/VLOSE).⁶⁴ Proporciona un canal seguro, y opcionalmente anónimo, para comunicar a la Comisión información interna (como informes, notas, intercambios de correos electrónicos, métricas de datos, investigaciones internas, decisiones y otras circunstancias pertinentes, ya sean pasadas, presentes o futuras). Sin embargo, el alcance de la denuncia se limita a las prácticas que incumplen las obligaciones de la DSA, como la moderación de contenidos, el funcionamiento de los sistemas recomendados, la publicidad, la evaluación y mitigación de los riesgos relacionados con los derechos fundamentales de los usuarios, las preocupaciones de seguridad y salud públicas, el discurso civil, los procesos electorales y los derechos de los niños. Si bien las plataformas digitales mejoran la accesibilidad y la eficiencia de la presentación de denuncias, su limitación radica en ofrecer denuncias sobre una gama limitada de temas. Además, su uso y eficacia dependen en gran medida de la aceptación y la confianza del usuario en el sistema.

5.2.3 ENCUESTAS EMPÍRICAS: EXPERIENCIAS POLACAS E ITALIANAS

En diciembre de 2022 se llevó a cabo una encuesta empírica entre profesionales, gerentes y directores de RRHH en Polonia, antes de la entrada en vigor de la Ley de Denuncia de Irregularidades polaca el 25 de septiembre de 2024. La encuesta se centró en la denuncia de irregularidades en el contexto más amplio del riesgo de personal, examinando las actitudes de los directivos hacia el riesgo, las fuentes de riesgo de personal, la eficacia de los sistemas de cumplimiento de RRHH (incluidos los mecanismos de denuncia de irregularidades) y los comportamientos y pérdidas relacionados con los riesgos del factor humano. La recolección de datos empleó los métodos de Entrevista Web Asistida por Computadora (CAWI) y Entrevista Telefónica Asistida por Computadora (CATI). Se aplicaron análisis estadísticos, incluyendo la prueba de chi-cuadrado con corrección de Yates y la prueba de Kruskal-Wallis, para evaluar las diferencias en las evaluaciones de los procesos de denuncia de irregularidades en función de variables como el puesto de trabajo, el tamaño de la empresa, la forma de propiedad y el sector industrial.⁶⁵

Los principales resultados de la encuesta polaca son los siguientes:

- A. La denuncia de irregularidades es ampliamente considerada como una herramienta importante tanto para detectar irregularidades en las organizaciones como para una gestión eficaz del cumplimiento.⁶⁶
- B. Un tercio de los encuestados carecía de una opinión clara sobre la eficacia de los sistemas de denuncia de irregularidades bien establecidos.

⁶³ Comisión Europea. Herramienta de denuncia de irregularidades de la Ley de Servicios Digitales: Proporcione información privilegiada sobre plataformas en línea, <https://digital-services-act-whistleblower.integrityline.app>

⁶⁴ Comisión Europea. Supervisión de las plataformas en línea y los motores de búsqueda de muy gran tamaño designados en el marco de la Ley de Servicios Digitales, <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses#ecl-inpage-lqfbha7w>

⁶⁵ Winnicka-Wejs, A. "La denuncia de irregularidades como herramienta para el sistema de gestión de cumplimiento de RRHH: informe de encuesta". Documentos científicos de la Universidad Tecnológica de Silesia 2023. Serie Organización y Gestión n° 182, 2023, pp. 573-596. DOI: 10.29119/1641-3466.2023.182.34 <https://managementpapers.polsl.pl/wp-content/uploads/2023/12/182-Winnicka-Wejs.pdf>

⁶⁶ *Ibidem*.

- C. En las empresas medianas, los encuestados proporcionaron calificaciones más altas para los canales internos de denuncia y protecciones contra represalias en comparación con otras organizaciones. Las diferencias en las puntuaciones basadas en el puesto de trabajo pueden atribuirse a las variaciones en la cultura organizacional, la confianza de los empleados en la eficacia de los sistemas de denuncia, el alcance de las irregularidades denunciables y la idoneidad de los canales internos.

En promedio, los profesionales calificaron los sistemas de denuncia de sus organizaciones por debajo del resto. Los profesionales de RR.HH., gerentes y directores de RR.HH. no estuvieron de acuerdo en su evaluación del nivel existente de confianza de los empleados en el correcto funcionamiento y la fiabilidad de los sistemas de denuncia de irregularidades de sus empresas.⁶⁷

Un estudio empírico paralelo fue realizado en **Italia** por la Escuela Nacional de Administración (SNA) en el marco del proyecto "Formación para el Cambio. Administración abierta y modelos de formación innovadores para la implementación eficiente de la denuncia de irregularidades".⁶⁸ El objetivo era evaluar el impacto de los programas de formación del SNA en la percepción de la denuncia de irregularidades, dado su relativo arraigo en la cultura jurídica y organizativa italiana.

En el estudio italiano se empleó una metodología similar a la encuesta polaca, utilizando las técnicas CAWI y CATI. Los datos se recogieron de una muestra de profesionales de RRHH, directivos y funcionarios públicos, aplicando análisis estadísticos como la prueba de chi-cuadrado con corrección de Yates y la prueba de Kruskal-Wallis para examinar las diferencias en función del puesto de trabajo, la estructura organizativa y el sector.

Los principales resultados de la encuesta italiana son:

- A. La formación desempeña un papel crucial no solo en la difusión de la concienciación y el conocimiento sobre la denuncia de irregularidades, sino también en la transformación de la percepción pública de la misma.
- B. La confianza y las barreras culturales siguen siendo desafíos importantes a pesar de las protecciones legales.
- C. El papel de apoyo de las Organizaciones de la Sociedad Civil está subutilizado y no es muy conocido (antes de la capacitación solo el 13% de los encuestados era consciente de su rol, después de la capacitación el porcentaje subió al 46,6%).
- D. Los canales internos son menos preferidos (38% de los encuestados) y muchos favorecen la denuncia externa (61%) porque se considera más fiable, independiente y eficaz.
- E. Los principales incentivos para denunciar irregularidades son: protección contra represalias (74,2% mujeres, 67,9% hombres), garantías de confidencialidad (68,5% mujeres, 67% hombres), saber que la

⁶⁷ *Ibidem*.

⁶⁸ Donini, V. M., Lostorto, V., & Zamaro, N. (2022). *Formare per trasformare: l'impatto trasformativo della formazione sulla prevenzione della corruzione. Prime riflessioni*. *Rivista di diritto amministrativo – Amministrativamente*, 4(2022). <https://www.amministrativamente.com/index.php/formez/article/view/13339>

actividad denunciada será abordada (59,2% mujeres, 57,8% hombres) y saber que el problema que plantee se considera importante/grave (41,7% mujeres, 46,4% hombres).

- F. Una recompensa monetaria no se considera un incentivo significativo (solo 3,8% mujeres, 7,3% hombres).
- G. El estudio subrayó la necesidad de una mayor capacitación para aumentar la concienciación, promover la denuncia de irregularidades como un deber ético y mejorar las protecciones para generar confianza en el sistema.

Además, siempre con referencia a **Italia**, es interesante notar que la ANAC, la Autoridad Nacional Anticorrupción, presentó un cuestionario a entidades del sector público y privado con el objetivo de verificar las soluciones adoptadas en una fase de aplicación inicial de la legislación. En el sector público, el 62% de las entidades han puesto en marcha una plataforma informática dedicada específicamente a la adquisición y gestión de denuncias en forma escrita. El 38% no ha creado una plataforma y ha adoptado diferentes métodos de recepción de denuncias, como el correo electrónico certificado o el correo ordinario.

En este sentido, se destacan dos aspectos críticos:

- A. entre las entidades que no han adoptado la plataforma también hay grandes administraciones, que tendrían todas las herramientas, en términos de disponibilidad de recursos humanos y materiales, para establecer más fácilmente la infraestructura de TI.
- B. El correo electrónico certificado y el correo ordinario no constituyen métodos adecuados de recepción de denuncias, si no están asistidos por contramedidas específicas destinadas a mitigar el riesgo de divulgación indebida de datos.

Los mismos perfiles críticos señalados anteriormente también se encontraron en el sector privado: sólo el 56% de los sujetos, de hecho, activó la plataforma informática y aproximadamente el 64% declaró haber previsto la posibilidad de realizar denuncias orales. Además, es interesante notar que, en el sector privado, solo el 30% de las entidades declararon haber recibido denuncias de denuncias: esto es una señal de que el marco de denuncia de irregularidades es aún poco conocido y debe fomentarse aún más.

Tanto el estudio polaco como el italiano revelan que, a pesar de reconocer la importancia de la denuncia de irregularidades, los empleados a menudo carecen de confianza en la eficacia de los mecanismos de denuncia y temen represalias. Si bien las iniciativas de formación, como se observa en el estudio italiano, ayudan a mejorar la concienciación, las barreras culturales y las debilidades institucionales siguen obstaculizando el establecimiento de culturas sólidas de denuncia de irregularidades. Abordar estos desafíos requiere no solo marcos legales, sino también políticas organizacionales proactivas, una comunicación más clara y protecciones fortalecidas para fomentar una cultura de integridad y transparencia. Si bien los resultados de la encuesta no son representativos y no se pueden generalizar a nivel nacional, pueden ser útiles para los propietarios de empresas, gerentes,

profesionales de recursos humanos y oficiales de cumplimiento, que son partes interesadas clave responsables de implementar sistemas efectivos de denuncia de irregularidades en el lugar de trabajo.

5.2 ÍNDICE PARA LA EVALUACIÓN DE LA PROTECCIÓN DE LAS PERSONAS DENUNCIANTES (IEWP)

Algunos investigadores han desarrollado un **Índice para la Evaluación de la Protección de las Personas Informantes (IEWP**, por sus siglas en inglés), una herramienta digital para evaluar la **eficacia de los mecanismos de protección** en diferentes países y períodos de tiempo.

El IEWP consta de subíndices cuantitativos y cualitativos. **El primero evalúa** las salvaguardas institucionales a través de indicadores, como la seguridad laboral, la confidencialidad, la protección contra represalias, la inmunidad legal, los índices de protección de las personas informantes (número de solicitudes de protección en comparación con las denuncias de corrupción, etc.). **El segundo se centra en capturar** las percepciones y experiencias relacionadas con la denuncia de irregularidades, incluidas las percepciones de diversos grupos (funcionarios, expertos, ciudadanos sin experiencia en la denuncia de irregularidades y los propios denunciantes) y las experiencias (solo de las personas informantes).

El IEWP permite comparar los niveles de protección de las personas informantes en distintos países y realiza un seguimiento de los cambios a lo largo del tiempo. Más allá de la medición, destaca las áreas clave de mejora, como la implementación oportuna de las leyes, la imparcialidad en el nombramiento de funcionarios y **la transparencia en la disponibilidad de datos**.

Los autores abogan por una metodología de dos pilares, que combine los datos administrativos con las respuestas a las encuestas, y hacen hincapié en la necesidad de estandarizar y mejorar el acceso a los datos pertinentes.

5.2.1 TRANSPARENCIA INTERNACIONAL

Tras la publicación de una metodología para evaluar la conformidad de los proyectos de ley con la Directiva de la UE sobre denunciante de irregularidades y las mejores prácticas,⁶⁹ Transparencia Internacional ha desarrollado un marco de autoevaluación para ayudar a las organizaciones a establecer, implementar y revisar sistemas internos de denuncia de irregularidades (IWS) que sean eficaces y estén en línea con las mejores prácticas y los estándares internacionales.⁷⁰ El marco incluye 130 preguntas que abarcan ocho dimensiones que van desde el alcance del sistema y la

⁶⁹ Transparencia Internacional. Evaluación de la legislación en materia de denuncia de irregularidades: metodología y directrices para la evaluación en relación con la Directiva de la UE y las mejores prácticas. 23 de septiembre de 2020, <https://www.transparency.org/en/publications/assessing-whistleblowing-legislation>

⁷⁰ Transparencia Internacional. Marco de autoevaluación del sistema interno de denuncia de irregularidades, <https://forms.office.com/Pages/ResponsePage.aspx?id=d2r57HSK7U-hwgM32S0wX1aBYjEGkwIJtPtUD4e4zFIUM0pCTTkwQVVkWFRRIN1kyTzU3UFVRREIMNy4u>

protección que proporciona, hasta la comunicación dentro del sistema y sobre él, y el seguimiento de su eficacia.⁷¹ Las preguntas están diseñadas para identificar factores potenciales que podrían socavar el IWS. Las respuestas y los hallazgos pueden ayudar a las organizaciones a mejorar la eficacia de su Sistema Interno de Alerta (SIA) en línea con las mejores prácticas y los estándares internacionales.

5.3 INDICADORES CLAVE PARA EVALUAR LOS SISTEMAS DE DENUNCIA DE IRREGULARIDADES

Sobre la base de las herramientas y los medios existentes, y teniendo en cuenta el estado y las necesidades de los sistemas de protección de las personas informantes en la UE y sus Estados miembros, esta sección tiene por objeto formular **un conjunto de indicadores cuantitativos y cualitativos** que puedan utilizarse para evaluar la eficacia de los mecanismos de denuncia de irregularidades.

Desde el punto de vista cuantitativo, los principales indicadores de evaluación se refieren principalmente al funcionamiento de los mecanismos de presentación de denuncias. Deben incluir, entre otros:

- A. Denuncias recibidas e informes fundamentados: el número total de denuncias recibidas y la proporción de las fundamentadas tras una investigación durante un período determinado (por ejemplo, anualmente).
- B. Inspecciones y sus resultados: número de inspecciones realizadas y sus resultados.
- C. Tiempos de respuesta/resolución: el tiempo medio que se tarda en confirmar, investigar y resolver problemas relacionados con las denuncias de irregularidades.
- D. Accesibilidad de los canales de denuncia: la disponibilidad de canales basados en el género, diversos y fáciles de usar (por ejemplo, formularios en línea, líneas directas, opciones cara a cara), su usabilidad en diferentes grupos demográficos y el respeto de la igualdad de género.
- E. Procedimientos judiciales y sentencias: el número de procedimientos judiciales iniciados, incluidos los procedimientos para poner fin a las acciones de represalia, y las sentencias dictadas durante un período específico (por ejemplo, anualmente).
- F. Incidentes de represalias y medidas de protección: el número de denunciantes que han sufrido represalias y las medidas adoptadas para hacer frente a estos casos (eficacia de la protección).
- G. Anonimato y confidencialidad: la existencia de medidas para proteger a las personas informantes y garantizar el anonimato.
- H. Acciones de seguimiento: la proporción (porcentaje) de casos que dan lugar a acciones correctivas o cambios en las políticas.
- I. Sanciones financieras y recuperaciones: montos cobrados por multas y otras sanciones financieras impuestas.
- J. Evaluación de los daños financieros: evaluación de las pérdidas financieras relacionadas con las malas conductas denunciadas.

⁷¹ Transparencia Internacional. *Sistemas internos de denuncia de irregularidades: marco de autoevaluación para organizaciones públicas y privadas*, 31 de octubre de 2024, <https://www.transparency.org/en/publications/internal-whistleblowing-systems-self-assessment-framework-public-private-organisations>

Los indicadores identificados proporcionan información mensurable sobre el rendimiento del sistema. Los métodos de recopilación de datos para estos indicadores pueden incluir:

- A Encuestas y cuestionarios distribuidos a los empleados y a las partes interesadas para medir el conocimiento, la confianza y la percepción de los sistemas de denuncias.
- B Análisis de estadísticas de informes, tasas de resolución y resultados de protección, estadísticas judiciales y métricas relacionadas (análisis de datos).
- C Evaluación del cumplimiento de la legislación y directrices en materia de denuncia de irregularidades, normas internas y políticas (auditorías de cumplimiento).

En países como **Bulgaria**, donde es difícil medir la eficacia del sistema de denuncia de irregularidades debido al bajo número de denuncias y casos judiciales, el enfoque debe cambiar hacia la creación de confianza a través de experiencias positivas y transparencia. La rapidez de acción tras una denuncia y la garantía de confidencialidad son clave para generar confianza en el sistema y animar a más empleados a utilizarlo. Si los empleados ven que las denuncias conducen a resultados reales y que la identidad de los denunciantes se mantiene confidencial, estarían más motivados para participar.

Por lo que se refiere a la retroalimentación cualitativa, la atención debe centrarse en enfoques indirectos o anónimos, como encuestas agregadas, investigación documental o canales seguros de retroalimentación que garanticen la confidencialidad y la protección de las personas informantes. Entre ellas se encuentran:

- A Los *focus group* se llevaron a cabo por separado con los empleados y las personas informantes para explorar las experiencias con el sistema y las actitudes culturales hacia la denuncia.
- B Casos de estudio:
 - I Análisis del marco de protección de los las personas informantes, incluido el cumplimiento de la Directiva de la UE, la legislación nacional, las normas y procedimientos internos (cumplimiento legal), así como la disponibilidad de apoyo psicológico, asistencia jurídica y otras medidas para las personas informantes (mecanismos de apoyo).
 - II Análisis de informes específicos de las personas informantes para evaluar el manejo de procesos y los resultados.
 - III Análisis de los ingresos financieros de las multas y sanciones, y evaluación de los daños financieros identificados.
- C Entrevistas de las partes interesadas con actores externos, como organizaciones de la sociedad civil, asociaciones profesionales, sindicatos y reguladores, para explorar la colaboración y el impacto sistémico.

Para fomentar la denuncia de irregularidades y mejorar los sistemas de denuncia de irregularidades, se pueden recomendar herramientas adicionales, como:

- A. Publicar evaluaciones detalladas del rendimiento de los sistemas de denuncia de irregularidades y de la cultura de la denuncia.
- B. Recopilar comentarios periódicos de las personas informantes, los empleados y las partes interesadas para identificar las brechas.
- C. Utilizar los resultados de las evaluaciones para perfeccionar los mecanismos de presentación de denuncias, los programas de formación y los marcos de protección.

5.4 EVALUACIÓN DE LA CULTURA DE LA DENUNCIA

Una sólida cultura de denuncia es esencial para el éxito de los sistemas de denuncia de irregularidades.

En este sentido, son importantes los métodos para evaluar la confianza de los empleados en los canales de denuncia, su disposición a denunciar las infracciones y su percepción de la capacidad de respuesta de la dirección. En varios niveles de la UE, se reconoce que la confidencialidad, incluida la protección de la identidad de las personas informantes, es una forma fundamental y eficaz de animar a los empleados a denunciar problemas.⁷²

Para evaluar la participación en la cultura de denuncia de irregularidades, se puede utilizar una serie de herramientas que evalúan la concienciación de los empleados, su confianza en el sistema de protección de las personas informantes, la frecuencia de las denuncias, etc.:

- A. La proporción de empleados que conocen los mecanismos de denuncia y sus derechos como informantes puede utilizarse para evaluar la concienciación de los empleados.
- B. Encuestas para medir la confianza de los empleados en la respuesta de la organización a las denuncias de irregularidades.
- C. La disposición y capacidad de los empleados para informar.

Herramientas como las encuestas y los grupos de discusión también se pueden utilizar para identificar las barreras para hablar y para apoyar estrategias para crear un entorno abierto y de apoyo para las personas informantes:

- A. Las encuestas o entrevistas con los directivos sobre sus percepciones sobre la denuncia de irregularidades y la transparencia de las denuncias pueden proporcionar información sobre las actitudes de la dirección y el liderazgo.
- B. La confianza de las partes interesadas externas en el compromiso de la organización con la protección de las personas informantes es una medida de la confianza pública.
- C. Los comentarios de las personas informantes sobre la imparcialidad y la transparencia de las investigaciones son un indicador importante del nivel de satisfacción con la resolución de los problemas de denuncia.

⁷² Supervisor Europeo de Protección de Datos (SEPD). Directrices sobre el tratamiento de información personal dentro de un procedimiento de denuncia de irregularidades, diciembre de 2019, https://www.edps.europa.eu/sites/default/files/publication/19-12-17_whistleblowing_guidelines_en.pdf?utm_source=chatgpt.com

Para garantizar una concienciación generalizada, es esencial:

Sensibilizar al público: por ejemplo, las partes interesadas de **Italia** revelan ideas interesantes sobre este tema. Con el fin de difundir una cultura de denuncia de irregularidades en la sociedad, el mensaje de denuncia debe transmitirse a través de medios que puedan llegar a un público más amplio. Para fomentar una cultura de denuncia de irregularidades, se sugiere que la Lega Serie A podría utilizar sus grandes afluentes de público dominicales para lanzar una campaña de concienciación y "actuar como portavoz en un tema tan sensible, como lo ha hecho en otros temas como la discriminación, el abuso, el feminicidio, etc.". Otra sugerencia es desarrollar elementos clave de comunicación para evaluar la percepción pública de la denuncia de irregularidades, tales como: la cultura de la denuncia, el periodismo comunitario, el periodismo de soluciones, el servicio público y los problemas colectivos. Para otros, la idea de la denuncia de irregularidades debe verse como una libertad democrática, una de las manifestaciones de la democracia que debe defenderse junto con la libertad de expresión. Además, la definición de denuncia de irregularidades como una forma de libertad de expresión se considera una innovación importante en el marco jurídico de la denuncia de irregularidades. También se propone un enfoque interesante para contrarrestar la cultura del silencio y establecer una nueva ética: aumentar la responsabilidad de los ciudadanos, difundir la conciencia de que denunciar irregularidades es una elección personal, reforzando la comprensión de que el/la denunciante es una persona común que hace algo ordinario. Además, se hizo hincapié en la necesidad de crear una cultura que hiciera que el sistema fuera cada vez menos institucional, por ejemplo, empoderando a los ciudadanos para que asumieran responsabilidades, ya que una cultura de desresponsabilidad o irresponsabilidad podría dar lugar a una avalancha de denuncias difamatorias o falsos elaborados para beneficio personal, abrumando los sistemas de presentación de denuncias.

Las partes interesadas en **España** expresaron la necesidad de cambiar la cultura y la mentalidad de que las personas informantes no son informantes sino colaboradores, de ver a las personas informantes como una fuente inteligente de información y de mostrar a los y las posibles denunciante que denunciar no es inútil y que es necesario generar confianza en el proceso.

Desde **España** surgió una cultura generalizada del silencio, impulsada por el miedo a las represalias y la exclusión del grupo, que se puede ver en el lugar de trabajo de manera similar a los niños en la escuela, donde cualquiera que señale un comportamiento inapropiado es visto como un soplón.

En **Bulgaria** se ha puesto de manifiesto que la cultura de la denuncia de irregularidades parece estar poco desarrollada y que el personal tiene poco interés o confianza en utilizar el sistema. Los entrevistados compartieron la idea de que una cultura de denuncia de irregularidades segura debe estar respaldada por mecanismos de confianza con una evaluación periódica de

la eficacia del sistema. Los encuestados argumentaron que mejorar la confianza y la eficacia del sistema requeriría una retroalimentación continua, supervisión y ajuste de los procedimientos. Las sugerencias incluyeron la realización de revisiones periódicas de las políticas internas y el intercambio de experiencias con otras organizaciones para mejorar la cultura general de denuncia de irregularidades.

Según los abogados en ejercicio en **Bulgaria**, es necesario establecer un vínculo claro, tanto en la legislación como en la práctica, así como en la comprensión pública, entre la protección de la libertad de expresión en los casos de SLAPP (Demandas Estratégicas contra la Participación Pública) y la protección de las personas informantes. Hasta ahora, esta interpretación no es visible en la legislación de la UE, la legislación nacional, la práctica jurídica y la comprensión pública. Los profesionales del derecho están tratando de incorporar aspectos del concepto SLAPP y de la legislación de protección de las personas informantes en la defensa en los casos de difamación. Si bien algunas jurisdicciones han mostrado interés en este enfoque, los resultados siguen siendo inciertos debido a la ausencia de jurisprudencia establecida. No obstante, se espera que algunos de los resultados de estos casos se aclaren en un futuro próximo.

Explorar las percepciones y la aceptación de las partes interesadas puede proporcionar información importante sobre el estado de la cultura de denuncia y ayudar a transformar una cultura de silencio en una cultura de denuncia activa.

5.5 EVALUACIÓN DE LA PARTICIPACIÓN Y COLABORACIÓN DE LAS PARTES INTERESADAS

Las partes interesadas desempeñan un papel fundamental en el éxito de las iniciativas de denuncia de irregularidades, desde el apoyo a las políticas hasta la actuación en relación con los problemas denunciados. Por lo tanto, es importante utilizar métodos adecuados para evaluar la eficacia de la colaboración de las partes interesadas, centrándose en la comunicación, la armonización de las políticas de denuncia de irregularidades y los esfuerzos conjuntos de sensibilización. Se puede utilizar un conjunto de indicadores para medir la colaboración de las partes interesadas.

Los indicadores sugeridos pueden medir:

- A. Frecuencia de participación: número de sesiones de formación conjuntas, campañas de sensibilización o foros con otras partes interesadas.
- B. Recursos compartidos: existencia y uso de asociaciones para obtener recursos compartidos (por ejemplo, asistencia jurídica, herramientas de investigación).
- C. Desarrollo colaborativo de políticas: involucrar a las partes interesadas en el desarrollo de políticas o directrices para personas informantes.

Se pueden utilizar varios métodos para evaluar la participación y la colaboración de las partes interesadas en las iniciativas de denuncia de irregularidades, entre ellos:

- A. Encuestas colaborativas para evaluar la satisfacción de las partes interesadas con las iniciativas conjuntas, proporcionando información sobre sus percepciones de la eficacia y las áreas de mejora.
- B. Análisis de redes para mapear el flujo de información y recursos entre las partes interesadas e identificar fortalezas y brechas en la comunicación y el intercambio de recursos.
- C. Análisis de resultados para medir el impacto tangible de los esfuerzos de colaboración, como el aumento de las denuncias de irregularidades o los casos resueltos.

PERSPECTIVA DE GOBIERNO ABIERTO

La recopilación periódica de datos y el análisis de las actividades de denuncia de irregularidades son clave para evaluar la eficiencia del sistema. Indicadores como los que se mencionan en este capítulo deberían informar en última instancia el ajuste de las políticas. Los principios del gobierno abierto sugieren que:

- A. Los datos siempre se publican en **estándares de datos abiertos**;
- B. La recopilación de datos y la transparencia incluyen información sobre **los procedimientos políticos y los procesos de participación de las partes interesadas**;
- C. Los hallazgos se comunican de manera transparente y se discuten con las partes interesadas, lo que garantiza que **los conocimientos impulsen mejoras accionables** que puedan diseñarse conjuntamente en el marco de un compromiso del Plan de Acción Nacional o como un reto de gobierno abierto independiente, que permite que se asuman y reconozcan compromisos de reforma ambiciosos fuera del ciclo regular del Plan de Acción.

En resumen, para mejorar y hacer más transparentes las evaluaciones periódicas de la eficacia de los sistemas de denuncia de irregularidades, la cultura de denuncia y la participación de las partes interesadas, se recomiendan los siguientes requisitos mínimos:

- A. Publicación periódica, al menos una vez al año, de evaluaciones detalladas de la eficacia del sistema de denuncia de irregularidades y de la cultura de la denuncia.
- B. Recopilación periódica de comentarios de las personas informantes, empleados y partes interesadas para identificar brechas y áreas de mejora.
- C. Utilización de los resultados de la evaluación para perfeccionar los mecanismos de presentación de denuncias, los programas de capacitación y los marcos de protección.

En conclusión, si bien el marco jurídico de la denuncia de irregularidades existe a nivel europeo y nacional, a menudo faltan la infraestructura y las medidas prácticas necesarias para su aplicación efectiva. El principio de gobierno abierto requiere la creación de un mecanismo institucional, ya sea una nueva institución o una existente, para apoyar la aplicación plena, justa y responsable de la legislación de denuncia de irregularidades, ayudar a las personas en situaciones difíciles, encontrar soluciones razonables y, en general, contribuir a la mejora tanto de la legislación como de los sistemas de denuncia.

5.6. RECOMENDACIONES

¿Qué se puede recomendar en base a los estudios empíricos?

1. REALIZAR ESTUDIOS EMPÍRICOS PERIÓDICOS EN LOS ESTADOS MIEMBROS

Teniendo en cuenta el estudio empírico llevado a cabo en Polonia (2.3), puede recomendarse que se lleven a cabo estudios similares de forma periódica en todos los Estados miembros con el fin de recopilar datos pertinentes y acumular conocimientos teóricos y empíricos sobre la percepción y la eficacia de los sistemas de denuncia de irregularidades en diferentes contextos organizativos y nacionales. Esto permitiría supervisar el desarrollo de los sistemas y mejorar continuamente su eficacia.

2. ADAPTAR EL ÍNDICE DE EVALUACIÓN DE LA PROTECCIÓN DE LAS PERSONAS INFORMANTES (IEWP)

El Índice de Evaluación de la Protección de las Personas Informantes– IEWP (2.4) puede ser tenido en cuenta y adaptado por los Estados miembros cuando desarrollen sus propios indicadores de evaluación. Si bien el IEWP se basa en la investigación del sector público, se puede adaptar para rastrear y evaluar las denuncias de irregularidades en los sectores privado y sin fines de lucro, cubriendo así de manera efectiva todas las formas de corrupción y mala praxis institucional.

3. APLICAR LAS RECOMENDACIONES CLAVE DE TI PARA SISTEMAS INTERNOS

A la hora de establecer y mantener un sistema interno de denuncia de irregularidades, es necesario tener en cuenta algunas recomendaciones clave de TI (2.5). Entre ellas se incluye garantizar que el sistema cumpla con los requisitos legales nacionales (leyes de protección de las personas informantes y otras leyes pertinentes, como la protección de datos o la legislación laboral), que sea inclusivo y tenga en cuenta las cuestiones de género, que se revise formalmente al menos una vez al año y que se realicen los cambios adecuados para mejorar su eficacia.

PERSPECTIVA DE GÉNERO

La recopilación periódica de datos y el análisis de las actividades de denuncia de irregularidades son clave para evaluar la eficiencia del sistema. Aunque las mujeres tienden a condenar el comportamiento corrupto más que los hombres, **parecen denunciar la corrupción con menos frecuencia que los hombres**, como lo confirman los datos del Barómetro Global de la Corrupción (GCB) de Transparencia Internacional⁷³.

Algunos **hallazgos clave** de diferentes investigaciones:

- A. Solo el **48 por ciento de las mujeres cree que puede denunciar actos de corrupción sin riesgo** de represalias, en comparación con el 54 por ciento de los hombres⁷⁴.
- B. **Incentivos para denunciar: una encuesta experimental realizada a más de 2.000**⁷⁵ empleados mostró cómo las mujeres están más incentivadas que los hombres para tomar medidas si existen **protecciones contra las represalias y obligaciones legales**.
- C. Según un estudio realizado en Italia⁷⁶, no hay diferencias significativas en la disposición a informar entre hombres y mujeres. Sin embargo, lo que hay que explorar más a fondo es el **miedo a las represalias de los directivos y colegas**, y el **aumento del estrés** que experimentan las mujeres después de denunciar.

En general, parece que entre los sujetos entrevistados para esta guía, hay una tendencia a no considerar las dificultades y complejidades de "**hablar**" para las mujeres, sino más en general para cualquier grupo marginado. Sin embargo, si los datos muestran que las mujeres tienden a hablar menos y sufren más por miedo a las represalias, esto **debería servir como un indicador** de la eficacia del sistema.

Recomendamos:

- A. **Tematizar el tema de las mujeres que sufren más daño** y represalias que los hombres
- B. **Sensibilizar sobre un enfoque inclusivo** a todas las diversidades y grupos más débiles que puedan estar presentes en una cultura organizacional
- C. **Sensibilizar sobre los casos** de sextorsión y acoso sexual. (Para explorar este tema más a fondo, consulte el recuadro del **Capítulo 1**).
- D. Publicación de datos desglosados **por género**, cuando estén disponibles: solo un pequeño número de organizaciones incluye datos sobre género y factores interseccionales. Esta brecha representa una **oportunidad perdida** para recopilar información actualizada que pueda respaldar la **toma de decisiones basada en evidencia**. Para abordar este problema, es esencial fortalecer los mecanismos de recopilación y análisis de datos, asegurando una comprensión más precisa del comportamiento, las necesidades y las prioridades de las personas informantes.
- E. **Capacitación y sensibilización sobre la denuncia de irregularidades con perspectiva de género**
- F. **Desarrollar un programa de formación dentro de la organización como medida preventiva**, destinado a educar a todos los miembros y participantes en las prácticas de denuncia de irregularidades, con un enfoque de género y la intersección de otros factores de vulnerabilidad, como la pobreza y los desequilibrios de poder. El programa debe abordar la denuncia de acoso, abuso sexual y conductas indebidas relacionadas con la corrupción, al tiempo que pone de relieve los diferentes efectos sobre las mujeres y los hombres, en particular la carga desproporcionada sobre las mujeres. También se debe hacer hincapié en la prevención de represalias, como el acoso sexual o la sextorsión, y en la sensibilización sobre los estereotipos de género, los prejuicios y las vulnerabilidades específicas que afectan a las personas informantes en situaciones marginadas.

CP. 1 >

⁷³ Barómetro Global de la Corrupción 2021 de Transparencia Internacional

⁷⁴ Barómetro Global de la Corrupción 2021 de Transparencia Internacional

⁷⁵ Ver: https://knowledgehub.transparency.org/assets/uploads/helpdesk/Gender-sensitivity-in-corruption-reporting-and-whistleblowing_2020_PR.pdf

⁷⁶ Donini, V. M., Lostorto, V., & Zamaro, N. (2022). Formare per trasformare: l'impatto trasformativo della formazione sulla prevenzione della corruzione. Prime riflessioni. Rivista di diritto amministrativo – Amministrativamente, 4(2022). <https://www.amministrativamente.com/index.php/formez/article/view/13339>

g Definir un MEL (Monitoreo, Evaluación y Aprendizaje) de las prácticas de denuncia de irregularidades con perspectiva de género:

- I** Implementar auditorías periódicas para garantizar que los sistemas de presentación de denuncias realmente mantengan la confidencialidad, el anonimato y la protección contra represalias, particularmente en casos basados en el género.
- II** Llevar a cabo evaluaciones de impacto con perspectiva de género para evaluar si las protecciones de las personas informantes apoyan efectivamente a las mujeres, las personas LGBTQ+ y otros grupos vulnerables.
- III** Establecer un mecanismo de retroalimentación en el que las personas informantes puedan informar de forma anónima de problemas con el sistema, garantizando la mejora continua.

Estas medidas ayudarán a evaluar la eficacia de las protecciones sensibles al género dentro del sistema de denuncia de irregularidades, garantizando que el sistema evolucione continuamente para proteger mejor a todas las personas informantes, en particular a aquellos que denuncian conductas indebidas basadas en el género.

6. RECOMENDACIONES SOBRE GÉNERO Y GOBIERNO ABIERTO

Capítulo 6

6.1 ENFOQUE DE GÉNERO

Es necesario aplicar de manera efectiva políticas públicas de protección de las personas informantes que integren **canales sensibles al género** tanto a nivel organizacional como externo. Es esencial abordar las lagunas de la normativa vigente, como la Directiva de la UE sobre la protección de las personas informantes de irregularidades y el marco jurídico nacional existente, que no tienen en cuenta explícitamente **los aspectos relacionados con el género**.

En este sentido:

- A. Los marcos regulatorios internacionales, nacionales y subnacionales deben reforzar las medidas para **establecer mecanismos de protección adaptados para las mujeres** denunciantes y otros grupos vulnerables
- B. Garantizar que **los canales de denuncia sean accesibles**, inclusivos y respondan a sus necesidades y riesgos específicos.
- C. Fortalecer los mecanismos de recopilación y análisis de datos para garantizar una comprensión más precisa del comportamiento, las necesidades y las prioridades de las personas informantes
- D. La aplicación **de canales sensibles a las cuestiones de género y políticas específicas** mejoraría la eficacia de los procesos de apoyo, en particular para las mujeres y otros grupos vulnerables. Garantizar que los procedimientos para denunciar, investigar y resolver quejas estén equipados para manejar las desigualdades interseccionales.
- E. **Reforzar las medidas de seguridad y confidencialidad con perspectiva de género en los sistemas de denuncia de irregularidades.** Garantizar que los sistemas de denuncia incluyan protecciones personalizadas para las conductas indebidas basadas en el género, salvaguardando el anonimato de las personas informantes y evitando represalias, especialmente en situaciones de desequilibrio de poder.
- F. Implementar protocolos de confidencialidad para asegurar las denuncias basadas en género, protegiendo las identidades y evitando la identificación indirecta.
- G. Desarrollar una **capacitación y sensibilización sobre la denuncia de irregularidades con perspectiva de género** como medida preventiva para educar a todos los participantes en las prácticas de denuncia de irregularidades, sobre el género y la intersección de otros factores de vulnerabilidad.

El programa debe:

- A. Abordar la denuncia de **acoso, abuso sexual** y mala conducta relacionada con la corrupción.
- B. Poner de relieve los **diferentes impactos sobre las mujeres y los hombres**, en particular la carga desproporcionada sobre las mujeres.
- C. Hacer hincapié en la **prevención de represalias**, como el acoso sexual o la sextorsión, y en la sensibilización sobre los estereotipos de género, los sesgos y las vulnerabilidades específicas que afectan a las personas informantes en situaciones marginadas.

6.2 LA PERSPECTIVA DE GOBIERNO ABIERTO (OG)

Hacemos un llamado a la implementación efectiva de políticas de protección de personas denunciantes que integren los principios de gobierno abierto, como la transparencia, la participación, la rendición de cuentas y la inclusión. Es esencial abordar las lagunas en las normativas y prácticas existentes, en particular cuando los sistemas de denuncia de irregularidades siguen siendo poco claros, inaccesibles o cuentan con un apoyo deficiente tanto de las instituciones como de la sociedad civil.

En este sentido:

- A. Los marcos internacionales, nacionales y subnacionales deben **reforzar la colaboración de múltiples partes interesadas para diseñar y monitorear conjuntamente los sistemas de denuncia de irregularidades**, combinando las perspectivas institucionales con las experiencias y conocimientos de las organizaciones de la sociedad civil (OSC), para garantizar la claridad, la accesibilidad y la confianza en el proceso de presentación de denuncias.
- B. Las partes interesadas institucionales y cívicas deben trabajar juntas para **garantizar que los canales de denuncia sean comprensibles, inclusivos y estén diseñados pensando en el usuario**, mediante el uso de un lenguaje sencillo, ejemplos prácticos e instrucciones claras a lo largo de todo el proceso de presentación de denuncias, incluida la orientación repetida y formularios fáciles de usar.
- C. Fortalecer los mecanismos de recopilación y análisis de datos sobre las prácticas de denuncia de irregularidades, garantizando que los datos se publiquen en formatos abiertos y se utilicen para **informar las políticas a través de diálogos transparentes con las partes interesadas y ciclos de mejora iterativos**.
- D. **Implementar sistemas de capacitación y apoyo para funcionarios públicos y responsables de denuncias internas**, yendo más allá de un enfoque puramente legalista para incluir el aprendizaje experiencial basado en dilemas éticos y simulaciones de casos de la vida real, en colaboración entre las autoridades públicas y las OSC.
- E. **Desarrollar campañas de comunicación conjuntas para aumentar la conciencia pública** sobre los derechos de **las personas informantes** y los servicios de apoyo disponibles, aprovechando los medios de comunicación nacionales, las plataformas culturales y los eventos deportivos para llegar a audiencias diversas.

- F. Promover análisis de riesgo participativos para identificar posibles áreas de mala conducta relevantes para la denuncia de irregularidades** dentro de las instituciones, involucrando tanto a los actores internos como a la sociedad civil para garantizar que los sistemas estén adaptados y sean sensibles al contexto.
- G. Establecer directrices sólidas de protección de datos elaboradas conjuntamente por las autoridades de protección de datos y las organizaciones de apoyo**, garantizando que los servicios de asesoramiento puedan procesar los datos personales de forma significativa y segura, equilibrando la privacidad con un apoyo eficaz.
- H. Diseñar conjuntamente nuevas leyes o regulaciones para ampliar los mecanismos de protección** para incluir no solo a **las personas informantes**, sino también a quienes los asisten, como las OSC de apoyo, los asesores legales y los periodistas, garantizando que estén protegidos de las represalias, en línea con las mejores prácticas internacionales y los marcos de derechos humanos.
- I. Crear y mantener registros públicos de centros de información cívica e institucional**, definiendo criterios claros de inclusión y fomentando la coordinación entre las organizaciones incluidas en la lista para referir a las personas informantes de manera efectiva y monitorear los desafíos sistémicos a través del intercambio regular entre pares.

MÁS ALLÁ DE LA GUÍA

Surgió un aspecto crucial: **el marco regulatorio** ha mejorado gracias a la directiva de la UE y su conversión en leyes nacionales, y otras reformas - algunas de ellas se incluyen en las recomendaciones al final de los capítulos anteriores- pueden mejorar aún más su impacto esperado en la buena gobernanza deseada.

Sin embargo, este compromiso **político "de arriba hacia abajo"** en materia de denuncia de irregularidades necesita bases sólidas para producir un impacto significativo en el **complejo** entorno social e institucional en el que surgen continuamente oportunidades para la corrupción y otras irregularidades. Esas bases se basan en valores, principios, expectativas, creencias: en otras palabras, la dimensión cultural es crucial para "empoderar" las normas informales y los juicios compartidos, alentando y apoyando socialmente la denuncia de irregularidades como un componente normal y valioso de una cultura deseable de **denuncia**. De hecho, los rasgos culturales que prevalecen dentro de ciertas organizaciones o sociedades tienen un impacto decisivo en la efectividad de cualquier implementación de **denuncias**. Especialmente en entornos donde la corrupción y las irregularidades se normalizan como reglas no escritas, la presión social contra las personas informantes puede ser la actitud dominante y exitosa. La cultura no se puede cambiar por decreto, obviamente, pero las reformas de la regulación formal proporcionan señales que abordan los cambios sociales: pueden "iniciar un proceso lento", que con el tiempo puede generar modificaciones profundas en la forma en que los individuos perciben y juzgan sus propias conductas y las de los demás. El dilema paradójico de la persona denunciante, si se presenta como "**héroe o traidor**", refleja precisamente la resistencia a **normalizar la práctica** de denunciar posibles irregularidades en interés público, fortaleciendo la conexión entre los enfoques "orientados a la denuncia de irregularidades" y "orientados a la persona informante", es decir, entre la dimensión formal/institucional y la perspectiva subjetiva y orientada a valores.

Para que la denuncia de irregularidades sea eficaz, hay que encontrar un equilibrio cuidadoso entre los intereses, las expectativas y los derechos contrapuestos de los diferentes actores que intervienen en el proceso, siendo la persona informante sólo uno de ellos. Los desafíos sustanciales asociados con cualquier marco regulatorio de denuncia de irregularidades se han destacado claramente en los capítulos anteriores. Cómo **minimizar los riesgos** de represalias, cómo salvaguardar los derechos a la privacidad y **proteger los datos sensibles**, cómo **verificar el contenido de las** denuncias de irregularidades, por ejemplo, son cuestiones complejas. Las innovaciones digitales presentan tanto oportunidades como desafíos: las plataformas en línea y las herramientas de comunicación segura pueden facilitar **la denuncia anónima** y mejorar la protección, pero también **plantean preocupaciones sobre la seguridad de** los datos y el potencial de uso indebido. Equilibrar los beneficios de las herramientas digitales con la necesidad de proteger la información confidencial es un **tema crítico**. En otras palabras, no se puede imponer aquí una fórmula universal y apta para todos: la regulación de la denuncia de irregularidades debe permitir a cualquier organización pública o privada, con sus propias características y antecedentes, adaptar su combinación particular y específica de contexto: fomento, restricciones, educación y aplicación de la ley.

La denuncia de irregularidades tiene un inmenso potencial como herramienta anticorrupción. Su efectividad, sin embargo, depende de que se aborden estos desafíos. Un análisis empírico en profundidad sobre los fundamentos morales y motivacionales de la denuncia de irregularidades parece una fuente de conocimiento necesaria para mejorar la **eficacia percibida** de las políticas correspondientes. Además, se debe explorar el papel de la formación ética y las herramientas educativas. Esta última, de hecho, debería ser eficaz para aumentar la congruencia de los valores de los individuos, en los que se socializan en los círculos de reconocimiento social dentro de las organizaciones públicas y privadas, con reglas y procedimientos orientados al interés público. Cuando **prevalece un cierto estigma social** hacia el papel de la persona informante, incluso las plataformas más sofisticadas para la denuncia confidencial o anónima serán inútiles. Una actividad perseverante de "**formación ética**" dentro de los aparatos públicos, así como de las organizaciones privadas, podría asumir un **papel crucial** en este sentido. Este compromiso debe estar dirigido a fortalecer los circuitos sociales de reconocimiento mutuo y el "**refuerzo**" **positivo** de la lealtad hacia los objetivos de las organizaciones públicas y privadas, consolidar las barreras morales contra la corrupción y las motivaciones éticas para denunciar las irregularidades.

En conclusión, parece necesario **replantear la dimensión social en la** que se están configurando a lo largo del tiempo las fuentes de reconocimiento moral, que son el principal motor de la decisión de "abrir el silbato". Después de todo, el éxito de la regulación y la legislación en materia de denuncia de irregularidades depende principalmente de su coordinación dentro de una acción colectiva anticorrupción más amplia "**desde abajo**", que involucre a todos los círculos sociales más importantes, tanto en el entorno laboral como en las esferas profesionales, asociativas, políticas, sindicales y religiosas. Solo esta última, de hecho, puede generar el fermento para un **cambio cultural**, es decir, un marco vinculante de creencias y normas informales donde se fomente y se apoye mutuamente la denuncia de irregularidades a través de la expresión pública de juicios éticos positivos sobre sus efectos socialmente beneficiosos.

ANEXO I: METODOLOGÍA DE LA INVESTIGACIÓN Y RECOGIDA DE DATOS

Esta guía es el resultado de la experiencia de cada socio en el campo y de una investigación realizada con métodos mixtos desde junio de 2024 hasta noviembre de 2024 en cuatro fases clave:

1. REVISIÓN DOCUMENTAL E INVESTIGACIÓN BIBLIOGRÁFICA

En esta fase se ha establecido un marco conceptual y regulatorio de protección de las personas informantes, evaluando las obligaciones, el nivel de implementación y las lagunas.

2. ANÁLISIS Y MAPEO DE LOS GRUPOS DE INTERÉS

En esta fase, se han identificado y mapeado cincuenta actores principales entre organizaciones de la sociedad civil (OSC), autoridades, sector privado, medios de comunicación, instituciones académicas y sindicatos. Esos son los actores que podrían influir o son importantes para promover la legislación y la concienciación sobre la denuncia de irregularidades. La base de datos de las partes interesadas ha sido la base para preparar una lista de organizaciones para la investigación cualitativa y las entrevistas.

3. ENTREVISTAS A INFORMANTES CLAVE EXPERTOS

En esta fase se ha entrevistado a representantes de al menos cinco organizaciones por país para recabar información sobre los desafíos, las oportunidades, las recomendaciones y las directrices. El guion de las entrevistas se ha basado en los temas de la guía, sin embargo, el método utilizado es la entrevista semiestructurada con informantes clave, para adaptarse a las respuestas de los entrevistados. Esto es particularmente útil para explorar prácticas innovadoras y completas que podrían no haberse considerado durante el diseño. Cada entrevistador ha recibido un acuerdo formal de consentimiento para cumplir plenamente con la protección de datos. Se han producido grabaciones de audio.

4. ANÁLISIS

Las entrevistas se analizaron utilizando un formato de resumen, que vincula el contenido de la entrevista a cada capítulo y destaca los siguientes temas clave:

- A.* Mejores prácticas existentes, ya sea implementadas por la organización entrevistada o citadas por ella.
- B.* Necesidades y desafíos identificados por el entrevistado en relación con el tema del capítulo.
- C.* Propuestas o puntos clave de actuación para mejorar la situación actual.

Además, los principales temas surgidos de las entrevistas, han sido recogidos y resumidos en un archivo excel.

ANEXO II: ACRÓNIMOS

ANAC: Autorità nazionale anticorruzione

CAWI: Entrevistas Web Asistidas por Computadora

CATI: Entrevista Telefónica Asistida por Computadora

CPDP: Comisión para la Protección de Datos Personales/ Комисия за защита на личните данни

OSC: Asociación de la Sociedad Civil

DPO: **Delegado** de protección de datos

DSA: Ley de Servicios Digitales

CEDH: Convenio Europeo de Derechos Humanos

UE: Unión Europea

GCB: Barómetro Global de la Corrupción de Transparencia Internacional

RGPD: Reglamento General de Protección de Datos

ONG: Organización no gubernamental

IEWP: Índice para la Evaluación de la Protección de las Personas Informantes

OAC: Oficina Antifraude de Catalunya

OCDE: Organización para la Cooperación y el Desarrollo Económicos

OG: Gobierno Abierto

OGP: Alianza para el Gobierno Abierto

SLAPP: Demandas Estratégicas contra la Participación Pública

SNA: Escuela Nacional de Administración

TFUE: Tratado de Funcionamiento de la Unión Europea

ONU: Naciones Unidas

UNODC: Oficina de las Naciones Unidas contra la Droga y el Delito

OMS: Organización Mundial de la Salud

WCAG: Pautas de accesibilidad al contenido web

W3C: Consorcio World Wide Web

WMS: Sistemas de Gestión de Denuncias



GUÍA DE INTEGRIDAD PARA INFORMANTES



Cofinanciado por
la Unión Europea