biblioteca COMPLIANCE

WORLD COMPLIANCE ASSOCIATION

biblioteca COMPLIANCE

07

GUÍA SOBRE CÓMO DISEÑAR UN CANAL DE DENUNCIAS EFICAZ EN ENTIDADES SIN ÁNIMO DE LUCRO

Junio 2024

La **World Compliance Association (WCA)** es una asociación internacional sin ánimo de lucro formada por profesionales y organizaciones interesadas en el mundo del *compliance.* La asociación tiene, entre sus objetivos, la promoción, reconocimiento y evaluación de las actividades de cumplimiento en las organizaciones (con independencia de su forma jurídica), así como el desarrollo de herramientas y procesos para una correcta protección frente a determinados delitos/infracciones cometidas por sus empleados, colaboradores o cualquier otra persona relacionada con ella.

La **Biblioteca Compliance** es un proyecto que tiene por objetivo desarrollar contenidos bajo un enfoque práctico a través de documentos de buenas práctica sobre cinco ejes principales alrededor del *compliance*:

Todos los documentos están disponibles en
www.worldcomplianceassociation.com

GUÍA SOBRE COMO DISEÑAR UN CANAL DE DENUNCIAS EFICAZ EN ENTIDADES SIN ÁNIMO DE LUCRO

Junio 2024

Guillermo González de la Torre Rodríguez
Coordinador de Estrategia y Calidad de Manos Unidas

Laura Gonzalvo Diloy
Directora de Auditoría Interna y Control de Riesgos de la FIIAPP

Patricia Fernández
Técnica del área Económica y Financiera de Medicus Mundi

Jorge Pelegrín Saenz
Técnico de Organización y Calidad de Confederación de Salud Mental

GUÍA SOBRE COMO DISEÑAR UN CANAL DE DENUNCIAS EFICAZ EN ENTIDADES SIN ÁNIMO DE LUCRO

Esta Guía pretende ofrecer orientaciones a todas aquellas entidades sin ánimo de lucro que deseen abordar el diseño del sistema interno de información, contemplado en la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, y del canal de denuncias que lo integra desde un enfoque eminentemente práctico.

El Comité ha partido de dos premisas para su elaboración, que han condicionado su contenido. Por un lado, consideramos que nuestras entidades deben ser más ambiciosas que la propia Ley y por ello hemos ampliado el ámbito de aplicación objetivo y subjetivo, como práctica que nos ayudará a fomentar la integridad y el respeto de los valores por parte de las personas que conforman nuestras organizaciones. Por otro lado, asumimos que el canal de denuncias es una herramienta fundamental para la detección y prevención de irregularidades, como pieza clave de cualquier programa de Compliance, pero para ello debe ser realmente eficaz y por tanto cumplir con una serie de requisitos.

A lo largo de este documento abordamos numerosas cuestiones y orientaciones para ser capaces de adaptar este nuevo reto a las necesidades de cada organización, porque no hay una única fórmula válida para todas. En este sentido, partiendo de un contexto previo muy necesario para la comprensión de por qué surge este desafío, ofrecemos una reflexión sobre el ámbito subjetivo y objetivo del Sistema Interno de Información, los principios que éste debe integrar, las fases que deben componer una debida gestión y tratamiento de las denuncias, así como las debilidades y oportunidades que ofrecen las diferentes alternativas para articular el canal de denuncias. Adicionalmente, se abordan cuestiones que nos ayudarán a interpretar la Ley, incluso en cuestiones que no están desarrolladas en la misma y que en cuyo caso se tratan de meras opiniones, en ningún caso vinculantes.

Este es el resultado del trabajo de diversas personas, que forman parte del Comité Técnico de Entidades Sin Ánimo de Lucro, y en el que hemos podido contar con la participación de Transparency International España en diversas fases del proyecto, organización que sin duda, nos ha aportado considerablemente gracias a su enorme conocimiento en la materia.

Laura Gonzalvo Diloy
Directora de Auditoría Interna y Control de Riesgos de la FIIAPP

biblioteca COMPLIANCE WORLD COMPLIANCE ASSOCIATION

ÍNDICE

CAPÍTULO 1: INTRODUCCIÓN (Guillermo González de la Torre Rodríguez): 08
- 1.1 Antecedentes y panorama actual 08
- 1.2 Obligatoriedad del canal de denuncias en las entidades sin ánimo de lucro 13
- 1.3 Legislación aplicable y relacionada 15
- 1.4 Definición y principales características de un canal de denuncias 17
- 1.5 Canal de denuncias, sistema interno de información y programa de cumplimiento: relaciones y diferencias 22

CAPÍTULO 2. PRINCIPIOS BÁSICOS PARA UN SISTEMA INTERNO DE INFORMACIÓN (Patricia Fernández): 26
- 2.1 Derechos de la persona informante, de la persona afectada y de otras terceras personas 34
- 2.2 Protección de datos personales 37

CAPÍTULO 3: ÁMBITO OBJETIVO Y SUBJETIVO (Guillermo González de la Torre Rodríguez): 41
- 3.1 Ámbito Objetivo 43
- 3.2 Ámbito Subjetivo 47

CAPÍTULO 4. FASES EN LA GESTIÓN DE DENUNCIAS EN UNA ORGANIZACIÓN (Laura Gonzalvo Diloy): 51
- 4.1 Comunicación de las denuncias 52
- 4.2 Recepción de las denuncias 55
- 4.3 Registro de la denuncia 59
- 4.4 Análisis preliminar de la denuncia 60
- 4.5 Investigación de la denuncia 64
- 4.6 Comunicación a la(s) persona(s) afectada(s) 66
- 4.7 Emisión del informe de la investigación 67
- 4.8 Resolución y cierre de la investigación 68
- 4.9 Comunicación a la autoridad competente 70
- 4.10 Rendición de cuentas 70

CAPÍTULO 5. *"PROS Y CONTRAS DE DIFERENTES ALTERNATIVAS DE CANALES DE DENUNCIA"* (Jorge Pelegrín Saenz): 72
- 5.1 Aspectos de la organización 72
- 5.2 Empecemos por el principio 73
- 5.3 Valoración de herramientas 77

GLOSARIO 79

CAPÍTULO 1. INTRODUCCIÓN

1.1 ANTECEDENTES Y PANORAMA ACTUAL

Guillermo González de la Torre Rodríguez
Coordinador de Estrategia y Calidad de Manos Unidas

A partir de la modificación del Código Penal en 2010 para introducir por primera vez en la historia de nuestra legislación el concepto de "responsabilidad penal de las personas jurídicas", hasta el día hoy, se han promulgado diferentes leyes, normas y guías que han encendido debates apasionados en aspectos relacionados con la manera en la que las entidades debían construir los programas o planes de cumplimiento normativo (o "compliance" en inglés). Es cierto que los principales elementos que debían contener esos programas quedaron definidos sin fisuras desde la segunda modificación del Código Penal en 2015 y tras la publicación de las instrucciones a los Fiscales por parte de la FGE en 2016[1]. Pero algunos matices sobre su implantación en el mundo real, y aún más en casos de entidades muy particulares, quedaron en cambio sin aclarar del todo. Algunas de estas dudas, pero solo a modo ilustrativo, pueden ser las siguientes:

- ¿En qué casos el comité de cumplimiento puede ser unipersonal o colegiado? ¿Cuál es el perfil que debe cumplir una persona de la organización para ser miembro de ese comité? ¿Debe ser una persona directiva? Y si no lo fuera, ¿cómo asegurar su autonomía para reportar directamente al órgano de gobierno? ¿Qué relación existe entre ese comité y los equipos que gestionan un canal de denuncias?

- El alcance de las irregularidades a vigilar y prevenir por un programa de cumplimiento, ¿basta con que sea hasta los delitos o infracciones penales? ¿Es necesario ampliarlo a toda conducta reprobable realizada por una persona relacionada con la organización? ¿Qué entendemos por reprobable? ¿Es todo aquello que contravenga una norma establecida, bien sea interna, sectorial o legal, incluyendo los procedimientos de una organización y su código de conducta?

- ¿Es obligatorio realizar, y cada cuánto tiempo, la evaluación formal de los riesgos de una organización a modo de una auditoría interna? ¿Qué papel debe asumir la persona responsable de llevarla a cabo con respecto a las demás figuras del cumplimiento dentro de la organización? Si la organización es pequeña, ¿pueden las mismas personas responsabilizarse tanto de prevenir incumplimientos a través de detectar y mitigar los riesgos a tiempo, como de actuar cuando el incumplimiento ya ha sucedido?

- ¿Cuál debe ser la configuración en la práctica de un canal de denuncias para la actuación en caso de recibir información sobre un incumplimiento? ¿Puede ser una cuenta de correo electrónico o sólo vale una aplicación informática específica? El equipo que lo gestiona, ¿puede ser unipersonal o colegiado; interno o externo? ¿Cuál es la diferencia entre un canal de denuncias y un sistema interno de información?

El objeto de la guía que tiene en sus manos no pretende aclarar y dar respuesta a todas estas dudas. La propia World Compliance Association (WCA) cuenta con un amplio catálogo de publicaciones que abundan sobre esos otros temas. Aquí nos limitaremos a tratar los elementos clave de un sistema interno de información, poniendo especial énfasis en los principios que lo rigen y el proceso en sí mismo de la gestión de las denuncias, entre otros temas. Y lo haremos además entendiendo un Canal de Denuncias dentro de ese Sistema Interno de Información, tal como señala la Ley 2/2023, el cual debe contar con otros elementos que integren plenamente el canal en el funcionamiento de la organización, y que será más sencillo o complejo conforme lo sea la propia organización. Procuraremos arrojar luz sobre cuestiones concretas como cuáles son las condiciones para asegurar que una denuncia sea eficaz e idónea. Cuáles son los principios fundamentales que una organización debe asegurar en el funcionamiento de un sistema interno de información. Cuáles son los elementos que deben formar parte de ese sistema y cómo son sus características más importantes. Cuáles son los derechos que asisten a las partes implicadas en una denuncia, así como la manera de garantizarlos. Quién y qué se debe o se puede denunciar, así como las principales actividades, objetivos y funciones que deben asumir las personas intervinientes en cada una de las fases del proceso de gestión de una denuncia. Cuál es el rol de la Autoridad Independiente de Protección del Informante y la relación que debemos tener con ella. Cómo son las fases de recepción, investigación y resolución de una denuncia, y cómo asegurar que queden bien diferenciadas, así como los plazos adecuados para cada una de ellas. Cuáles son las obligaciones a tener en cuenta sobre la conservación, la seguridad y la protección de datos personales. Y, por último, cuáles pueden ser las alternativas para

[1] Circular 1/2016, de 22 de enero, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015.

construir un canal de denuncias o un sistema interno de información según sea el tipo de organización que se trate, así como las ventajas y los inconvenientes de optar por un modelo o por otro. Eso sí, todo en forma de recomendaciones y descripciones generales que luego cada organización tiene que comprender y usarlas para hacerlas suyas y crear su propio canal de denuncias y sistema interno.

La base de toda esta guía es la interpretación de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. Este análisis ha sido realizado por un conjunto variado y experto de organizaciones que formamos parte del Comité de Compliance de Entidades Sin Ánimo de Lucro de la WCA, y por Transparencia Internacional. Para esa interpretación, lo primero que hicimos fue trazar un margen de maniobra suficiente donde incluimos los requisitos mínimos e irrenunciables sobre los límites que consideramos que marca esta Ley. A continuación, analizamos a fondo el concepto y el objetivo que debe perseguir un canal de denuncias y un sistema interno de información, relacionándolo con otras leyes similares, con experiencias prácticas que tenemos a mano, y con las exigencias éticas con las que trabajamos las entidades sin ánimo de lucro. Y como resultado de esa comparación, ampliamos el alcance del canal de denuncias y del sistema que recoge esa Ley, tanto en el ámbito subjetivo (quién puede denunciar)[2] como en el objetivo (qué se puede denunciar) . Por último, analizamos cómo se podrían afrontar las dificultades que se podrían encontrar las organizaciones más pequeñas o con menos recursos, durante su puesta en práctica.

A pesar de existir algunas imprecisiones e incertidumbres sobre cómo abordar este tema, creemos que estamos asistiendo por fin a un momento donde las dudas de prácticas muy concretas van a resolverse de una vez por todas. Porque hoy podemos afirmar que contamos ya con un cuerpo de experiencias probadas y abundantes a la hora de implantar un programa de cumplimiento normativo; indistintamente de su fin, tamaño, volumen de ingresos, tipo de actividad o personalidad jurídica. Desde esa primera modificación del Código Penal han pasado ya 14 años y eso ha permitido que organizaciones de toda condición pusieran en marcha sus propios sistemas, los cuales además se han ido actualizando desde entonces cada vez que ha surgido alguna iniciativa legal o recomendación sectorial. Un camino repleto de iniciativas muy solventes y exitosas que nos indican con claridad cuáles son las características que debemos tener en cuenta para construir nuestro canal de denuncias y nuestro sistema interno.

Por otro lado, si analizamos esta evolución, comprobaremos que el cumplimiento normativo nació como un programa más a añadir en una entidad y que, con el tiempo, se ha convertido en un sistema completo de gestión que se debe integrar en el normal funcionamiento de la misma. De tal modo, que alrededor de la gestión de los riesgos de incumplimiento se debería generar un conjunto de instancias con funciones propias, compuestas por personas que asuman una serie de actividades, las cuales producirán unos resultados concretos, con los que luego se podrán tomar las decisiones más adecuadas. Todos estos componentes, además, deben ser medidos y analizados para comprobar la eficacia del sistema y detectar la necesidad de su mejora continua.

Aunque parezca paradójico, esta necesidad de que se implante de forma integral en una entidad, lejos de arruinar la vida de las organizaciones más pequeñas o con menos recursos, permitirá que un programa de cumplimiento se pueda integrar junto a otras obligaciones transversales que ya tienen estas organizaciones. Esto les ayudaría a aprovechar y compartir los canales, los comités y las personas con los que cuentan de forma interna. Aunque, eso sí, habría que afrontar un nuevo esfuerzo de formación y de sensibilización sobre las especificidades de este tema, pero después de ese inicio, luego será más sencillo incorporar estas nuevas actividades a las que ya se realizan.

No obstante, estamos convencidos de los beneficios concretos que supone la implantación de un canal de denuncias en una organización sin ánimo de lucro, más allá de que sea obligatoria o no por ley. Si se analiza con perspectiva, se comprueba que lo urgente y lo básico saturan la agenda de los temas que puede abordar una organización en cada momento. Pero hay asuntos muy importantes que, al no dar un beneficio inmediato o evidente, no se atienden y se posponen sin remedio. Asuntos que ayudan a las organizaciones a mejorar y profesionalizar su gestión y a incorporar métodos que le eviten problemas o le hagan disminuir el tiempo que se necesita para cada tarea. Un canal de denuncias, en ese sentido, dota a una or-

[2] Ver capítulos 3 y 4 de esta guía sobre "Ámbito objetivo y subjetivo" y sobre "Fases de gestión de las denuncias", respectivamente.

ganización de un seguro eficaz contra el fraude y las malas prácticas.

Está comprobado por diversas teorías al respecto, que el delito aumenta de manera proporcional conforme crece la oportunidad de cometerlo con sencillez y sin consecuencias. De tal forma que un delito no solo lo cometerían personas con gran desesperación personal o falta total de escrúpulos, sino también personas en situación más corriente que no querrían desaprovechar esa oportunidad si se les presenta de ese modo. La manera más eficaz de disminuir esa posibilidad son los controles y los procedimientos, por un lado, pero también la concurrencia de testigos que vigilan de manera natural, y la facilidad que tengan esos testigos para denunciar lo que han visto. Un canal de denuncias es, por tanto, una de las herramientas que más contribuyen a la promoción de la ética dentro de una organización y, en consecuencia, a instaurar una cultura del cumplimiento. Si alguien sabe que hay un canal y que funciona correctamente, dejará de plantearse si le compensa o no el riesgo de cometer un delito. Algo que, en cascada, redundará directamente en la organización y en una manera de trabajar más responsable y diligente.

No ignoramos, en cualquier caso, que la labor de adaptación y de cumplimiento de obligaciones por la aprobación de una nueva ley, es siempre una tarea costosa en tiempo, dinero, reflexión y tensión interna que generan gran estrés y desgaste a cualquier organización. Organizaciones que ya están sometidas a abundantes exigencias administrativas y de gestión, además de la presión con la que viven por su mera supervivencia en un entorno tan competitivo y turbulento como el actual. Aún más, si nos referimos a las organizaciones con fin social y sin ánimo de lucro.

Es a todas ellas a las que va dirigida esta publicación. Con el convencimiento de que todo esfuerzo, por obligatorio que sea, pueda ser al menos afrontado con más claridad, certidumbre y orden. Para que nuestras organizaciones sin ánimo de lucro puedan centrar sus recursos en los nobles fines que persiguen y no distraigan demasiado su atención en resolver problemas que se podrían evitar con las recomendaciones que aquí les mostramos. Para que los análisis y las acciones que lleven a cabo en la construcción y mantenimiento de este canal de denuncias y sistema interno, los puedan utilizar también para su provecho y la mejora de su organización.

1.2 OBLIGATORIEDAD DEL CANAL DE DENUNCIAS EN LAS ENTIDADES SIN ÁNIMO DE LUCRO

El canal de denuncias, vistas las legislaciones en vigor hasta el momento, es obligatorio para todas las entidades del sector público indistintamente de su tamaño y nivel. Y lo es también para todas las demás personas jurídicas de ámbito privado que tengan 50 o más personas trabajadoras, indistintamente de su personalidad jurídica.

Aunque si la organización es un sindicato, un partido político o una organización empresarial, así como una fundación creada por ellos, entonces también será sujeto obligado si además recibe fondos públicos, indistintamente del importe de esos fondos y del número de personas contratadas.

También deberán cumplir la Ley aquellas entidades que entran dentro del ámbito de aplicación de leyes europeas sobre mercados financieros, prevención del blanqueo y financiación del terrorismo, seguridad del transporte, y protección del medio ambiente. En este otro caso, deberán comprobar que la normativa específica que les aplique incluya la exigencia de contar con un sistema interno de información, y que éste cubra todas las exigencias que tiene la Ley 2/2023 porque, si su normativa no las recoge, las deberá cumplir igualmente y añadirlas al sistema que ya haya puesto en marcha.

Aludiendo a esta última precisión, tenemos que las fundaciones y las asociaciones son sujetos parcialmente obligados de la Ley 10/2010 sobre prevención del blanqueo de capitales y de la financiación del terrorismo, a las que les aplica su artículo 39, así como su desarrollo concreto que recoge el artículo 42 del Real Decreto 304/2014. Los requisitos establecidos en esos artículos no exigen que se establezca un sistema interno de información al completo, sino sólo el requisito de informar en caso de sospecha o indicio de existir una infracción al respecto. En ese sentido, solo las fundaciones y las asociaciones con 50 o más personas trabajadoras, o para todas cuando éstas sean del sector público institucional, deberán cumplir la Ley 2/2023, pero lo deberán hacer integrando y diferenciando en su sistema interno de información aquellos hechos referidos a la ley de blanqueo y terrorismo.

Por otro lado, si una organización

se plantea poner en funcionamiento un canal de denuncias o un sistema interno de información, a pesar de no ser sujeto obligado de la Ley, ésta exige "*que deberá cumplir, en todo caso, los requisitos previstos en esta ley*[3]". Téngase en cuenta, además, que los planes de compliance, en su aplicación más completa, incluyen la necesidad de prevenir delitos a través de la evaluación de riesgos y de la puesta en marcha de medidas que los mitiguen, así como la de actuar en caso de recibir información sobre la ocurrencia de un delito, lo cual se realiza por medio de un canal de denuncias. En esos casos, ese canal que tenga la organización siempre tendrá que cumplir con todos los requisitos de esta Ley.

Así que, resumiendo y conocidas las especificaciones realizadas, podemos afirmar que las entidades sin ánimo de lucro propias de nuestro sector que están obligadas a contar con un canal de denuncias, integrado en un sistema interno de información, son las siguientes:

- Las fundaciones públicas.
- Todas las entidades privadas que tengan más de 50 personas trabajadoras: asociaciones, fundaciones, entidades religiosas, cooperativas y organismos especiales.
- Los sindicatos, partidos políticos y organizaciones empresariales, así como las fundaciones creadas por ellos, que reciben fondos públicos, indistintamente del volumen de su plantilla.

Ahora bien, conocida la obligación, lo determinante será la manera en la que una organización ponga en marcha ese canal. Y dada la amplia diversidad de las organizaciones de nuestro sector, será tan importante que el canal sea adecuado y eficaz, como que esté adaptado a las particularidades de cada una. Y para ello habrá que tener en cuenta el tamaño, la implantación geográfica, los recursos, la capacidad o especialidad de sus integrantes, la experiencia en temas similares, el nivel de riesgo de cada organización, y la naturaleza de su cultura e identidad, referida a su misión, visión y valores.

Por esa razón, para adoptar un canal de denuncias se pueden valorar opciones muy distintas que pueden ir desde la construcción y la asunción interna de un canal al completo a cargo de una unidad nueva que se constituya exprofeso en la organización, hasta la contratación conjunta por parte de varias entidades pequeñas de naturaleza similar, de una empresa externa que se responsabilice de gran parte de la gestión de ese canal, **o de que la gestión se lleve a cabo por cualquiera de ellos, respetando en todo caso las garantías previstas en la ley**. En ese sentido, la ley referida para la protección de las personas informantes establece que[4], siempre y cuando la entidad no supere las 250 personas en plantilla, éstas podrán compartir recursos y procedimientos con otras organizaciones, aunque se deberán diferenciar y tener en cuenta las especificidades de cada una.

1.3 LEGISLACIÓN APLICABLE Y RELACIONADA

De manera cronológica, la legislación aplicable a los canales de denuncia es la siguiente:

- Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Circular 1/2016 de la Fiscalía General del Estado, **de 22 de enero**, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015.
- Directiva (UE) 2019/1937 de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.
- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Aunque de un modo u otro, esta legislación también está relacionada con la promoción de la ética y de una cultura de cumplimiento, y aplica al sector de las entidades sin ánimo de lucro:

- Ley Orgánica 3/2007, del 22 de marzo, para la igualdad efectiva de mujeres y hombres.
- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

[3] Ley 2/2023, Art. 10.2: "*Las personas jurídicas del sector privado que no estén vinculadas por la obligación impuesta en el apartado 1 podrán establecer su propio Sistema interno de información, que deberá cumplir, en todo caso, los requisitos previstos en esta ley*".

[4] Preámbulo III y Artículo 12. Medios compartidos en el sector privado, de la Ley2/2023.

- Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de libertad sexual.
- Resolución de 18 de octubre de 2022, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de acción e intervención social 2022-2024.
- Ley 4/2023, de 28 de febrero, para la igualdad real y efectiva de las personas trans y para la garantía de los derechos de las personas LGTBI.
- Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.

1.4 DEFINICIÓN Y PRINCIPALES CARACTERÍSTICAS DE UN CANAL DE DENUNCIAS

Hechas las contextualizaciones y las salvedades, es conveniente ahora definir lo que consideramos que es un canal de denuncias:

> "La vía donde una persona informa a una organización de hechos ocurridos en su seno, que esa persona considera ilícitos, cuyo uso obliga a esa organización a proteger a la persona informante, a valorar la admisión de esos hechos a trámite, a investigarlos formalmente, si procede, con las garantías procesales correspondientes y solicitando la colaboración de las partes implicadas, y a adoptar y notificar una resolución final al respecto".

En este apartado, explicaremos cada uno de los componentes de esta definición, lo cual nos servirá para ofrecer una perspectiva general pero completa de lo que debe tener un canal de denuncias. Lo primero que queremos destacar es el concepto de "ilícito", que es toda conducta atribuible a una persona que es contraria a la ley y a las normas que afectan a una organización. En cuanto a investigar formalmente los hechos de los que se ha informado, este tiene el objetivo de comprobar si esos hechos son veraces y si incumplen o no la ley y/o la normativa que afecta a esa organización.

En caso de que los hechos sean veraces y de que además infrinjan una ley o una norma determinada, la organización procederá a aplicar la sanción correspondiente a la parte denunciada, que siempre será una persona física que mantiene una relación formal con esa entidad, bien sea una persona trabajadora, voluntaria, socia, proveedora, contraparte o beneficiaria. Esta relación formal se evidencia por el contrato o convenio firmado que se haya establecido entre ella y la organización. Si no existe vínculo alguno, la organización entonces no tendrá competencia sobre la misma y, por lo tanto, no podrá aplicarle ninguna sanción. Será conveniente entonces que la organización informe del caso, si procede, a la empresa o entidad donde trabaja esa persona y con ello se dé por cerrada la investigación.

Asimismo, la organización también ofrecerá la reparación, si procede, a la parte que sea víctima del hecho informado, con el objetivo de res-

taurar, en lo posible, el daño causado y de fortalecer la cultura ética y de cumplimiento de la organización.

Si volvemos a la definición, veremos que el canal deberá estar siempre abierto y accesible para que cualquier persona pueda informar, pero su uso no obliga a que dicha persona se identifique o a que, haciéndolo, se preste a participar en la investigación que corresponda. Tampoco está obligada a preparar esa información con más argumentos o pruebas que aquellas que tenga y que sea capaz de aportar. No debe ser una experta en la materia en cuestión, ni formular la denuncia con orden y precisión, aunque eso afecte luego a su admisión o al resultado final de la investigación. Por este motivo, en la definición empleamos el verbo "considerar" para referirnos a lo que esa persona informante cree de forma subjetiva que es oportuno denunciar. Porque para presentar una información, basta con que esa persona crea que ha sido testigo o sienta que ha sido víctima de una irregularidad. Aunque será luego la organización la que valore esa consideración suya para deliberar si eso realmente encaja con un hecho denunciable y en la manera en la que lo disponga el canal y el sistema en sí. La organización, en ese sentido, estará siempre obligada a valorar la información que remita esa persona y a responderle con criterio y de manera fundamentada, aunque la respuesta sea no abrir una investigación por no admitir su denuncia a trámite.

De manera análoga y siguiendo nuestra definición de un canal de denuncias, la persona que responda del hecho informado como infracción, y que podrá ser sancionada si el proceso concluye su responsabilidad, también podrá negarse a colaborar en la investigación. A pesar de que eso le pueda perjudicar en su capacidad de defensa. Por este motivo, en la definición recogemos que las obligaciones recaen en la organización, y que, a las personas implicadas, como mucho, se les "solicitará su colaboración", destacando en todo caso los derechos que les asisten a lo largo de todo el trámite que se lleve a cabo.

Desarrollando este aspecto concreto, tenemos que se podrían dar cuatro situaciones distintas:

1. Que la organización no admita a trámite la denuncia presentada, por no ajustarse a los términos de lo que considera una denuncia.

2. Que siendo admitida la denuncia, la persona informante no dé sus datos de contacto y, por tanto, sea imposible contactar con ella para realizar conjuntamente el proceso de investigación.

3. Que, aun dando sus datos, la persona informante decida no colaborar en ese proceso y no aporte más información que aquella que dio al inicio.

4. Que la persona acusada también decida no colaborar en ese proceso, sin personarse en las comparecencias que se le haga llegar, ni remita la información que se le solicite.

Las situaciones 2, 3 y 4 pueden mermar la posibilidad de contar con más información y evidencias que ayuden a demostrar la veracidad de los hechos, pero no afectan a la obligación que tiene la organización de llevar a cabo el proceso de investigación y de adoptar la resolución que corresponda. Insistimos, por tanto, en que, si la organización abre una investigación, ésta la deberá llevar a cabo siempre hasta el final, según unos plazos establecidos y las garantías procesales correspondientes, y notificando el resultado obtenido, indistintamente del éxito que pueda tener la investigación por no contar con suficiente información.

Hay que tener en cuenta además que, si no existen pruebas que demuestren que esos hechos ocurrieron o quiénes fueron los que cometieron esa infracción o que esos hechos sean realmente una infracción, el caso entonces se cerrará sin resultados concluyentes. Pero la información restringida de ese caso siempre constará en el canal para que pueda ser utilizada de alguna forma, si aparecieran nuevos indicios o casos similares en el futuro que las circunstancias en esa ocasión permitan relacionarlos entre sí.

Por otro lado, si una persona no quiere dar sus datos personales, el canal tendrá que ofrecer la posibilidad de que la persona informante pueda contactar y recibir la información de su caso sin que sea revelada su identidad en ningún momento, ni quede rastro de la misma.

El soporte más común y seguro para habilitar un canal es una aplicación informática específica a la que se accede a través de la web de la organización. Sin embargo, para garantizar el anonimato y la confidencialidad de la persona informante, así como el acceso universal al canal, también se podrán poner en marcha medios alternativos para aquellas organizaciones y grupos de interés que no pueden o no quieren

usar Internet. Estos medios pueden ser buzones físicos, teléfono o incluso encuentros presenciales de la persona informadora con las personas responsables del canal o también con las personas representantes autorizadas del canal, las cuales pueden denominarse "puntos focales".

Esta condición asimétrica del flujo de la comunicación entre las partes que participan en un canal de denuncias es la que permite que las personas puedan informar de manera anónima, que es una de las características esenciales para lograr que dichos canales sean eficaces. Como veremos en el capítulo referido a ellos, tres de los fundamentos para construirlos adecuadamente son la accesibilidad, la confidencialidad y la protección de la persona informante. La prioridad de fondo en todo ello es que el canal sea ampliamente usado y que nunca se convierta en una barrera de entrada para la persona que vaya a informar. Que jamás se pierda información valiosa que la organización podría emplear para prevenir irregularidades y actuar diligentemente. Porque si la persona informante percibe que no es un canal seguro, o que no sirve para nada, o que su activación es compleja, larga o confusa, el canal acabará finalmente en el olvido.

Por eso es tan importante que quede claro desde el principio, que detrás de la gestión del canal existirá/n una/s persona/s responsable/s, debidamente cualificada/s, así como un equipo o comisión de investigación/instrucción que investigará los casos recibidos. Que estas personas serán nombradas formalmente para esta función y que su perfil profesional estará relacionado con el control, la inspección o la asesoría. Personas que podrán ser auditoras internas, supervisoras de gastos, expertas jurídicas o responsables de prevención, calidad, organización o planificación. Si se hace percibir que existe esta estructura formal y competente, se logrará asegurar al público que estas personas extremarán su diligencia en el manejo de la responsabilidad tan delicada que asumen con la gestión del canal de denuncias.

En cualquier caso, si se da a entender por descuido o por cualquier otra razón, que las informaciones recibidas se han abordado con ligereza, que no se han cumplido los plazos previstos, que se ha podido quebrar la confidencialidad, que pueden derivarse inconvenientes o represalias internas por el solo hecho de usar el canal, que no se ha recopilado toda la información que sea necesaria, que la organización se ha movido influenciada torticeramente de algún modo por el riesgo reputacional que conlleva la acusación o el peso institucional de la persona denunciada, entonces el canal dejará de ser eficaz, y será muy difícil que lo haga alguna vez. Por no hablar de que, si se demostrara tal falta de diligencia, la organización sería objeto de una sanción importante por falta grave.

Por eso, y para asegurar un proceso con todas las garantías, la organización deberá asignar recursos, funciones, poderes, tiempo y formación de manera suficiente a las personas que intervendrán en él. Todo ello regulado mediante procedimientos completos y claros que se deberán seguir a rajatabla. Además, el órgano de gobierno deberá firmar una política que eleve el compromiso de la organización a su máximo nivel, junto con un régimen sancionador que establezca el tipo de faltas que existen, cuáles son las condiciones para estimar unas y otras, y cuáles son las sanciones que la organización impondrá según sea la falta.

Como vemos, el éxito de la implantación de un canal de denuncias está en juego desde el primer día. Cuando se proceda al lanzamiento del canal y se realicen acciones de difusión externa y de formación interna, deberá destacarse cómo estos aspectos esenciales han sido tenidos en cuenta en su construcción y evidenciarlos con referencias concretas a las características del canal. También deberá explicarse bien cuál es su funcionamiento y describir cuáles son los pasos concretos a seguir en cada fase del proceso.

Asimismo, otro punto crucial será también el abordaje del primer caso o denuncia que se reciba. Es el momento en el que la/s persona/s responsable/s del canal y el comité investigador aplicarán los procedimientos correspondientes y comprueben en directo el nivel de dominio y de preparación que tenían. Por este motivo, será muy importante que la organización priorice este tema durante ese estreno, y dedique toda su atención a ese primer caso, con el objetivo de que se proceda según lo previsto.

Para mitigar la posibilidad de errores o dificultades a la hora de interpretar y aplicar lo que señalen esos procedimientos, se recomienda que esas personas reciban formación específica sobre este tema y que en esa formación se incluya una sesión de ensayo o de simulacro sobre el funcionamiento de ese canal.

1.5 CANAL DE DENUNCIAS, SISTEMA INTERNO DE INFORMACIÓN Y PROGRAMA DE CUMPLIMIENTO: RELACIONES Y DIFERENCIAS

Para finalizar esta introducción, queríamos abordar una de las dudas más recurrentes que nos ha llegado. Al aparecer en España la Ley 2/2023 mucho más tarde que el desarrollo normativo sobre la "responsabilidad penal de las personas jurídicas", ha habido tiempo para que se pusieran en marcha distintos programas de cumplimiento que, entre sus principales componentes, se encuentra el canal de denuncias. Lo que exige esta Ley, sin embargo, es algo más que un canal ya que habla de un sistema interno de información donde detectar y gestionar infracciones legales graves. En concreto, infracciones administrativas graves o muy graves, infracciones penales e infracciones contra el Derecho de la Unión Europea, especialmente en aquello que afecte a sus intereses financieros, la competencia y ayudas otorgadas por los Estados, el mercado interior y la fiscalidad de las empresas.

Asimismo, la Ley en sus motivaciones pone a la persona informante en el centro, y desarrolla a su alrededor la forma en la que se garantice su confidencialidad o su anonimato, y que su acción de informar no le genere consecuencias negativas en la organización para la que trabaja. Por eso, insiste en las medidas de protección y habilita una Autoridad Pública Independiente que contará a su vez con su propio sistema de información.

Este giro de su enfoque hacia la persona informante busca la manera de incrementar las denuncias que puedan provenir de la actividad económica más habitual. Su prioridad no es tanto la organización, sino la persona que informa. Están convencidos de que la denuncia desde dentro de los espacios comunes de trabajo, es la vía más efectiva para hacer aflorar los fraudes, el soborno y la corrupción. Ya había leyes similares que responsabilizaban parte de esta tarea a las organizaciones, pero con esta nueva ley parecen indicar que el esfuerzo al respecto no estaba siendo suficiente y que había que exigirles que hicieran algo más desde la perspectiva del informante a propietarios, accionistas, administradores y representantes legales de las distintas personas jurídicas que existen.

Hasta el momento antes de esta Ley, un canal de denuncias al uso se había configurado al servicio de los intereses de una entidad. Un mecanismo para proteger su patrimonio y el de sus personas administradoras, por los delitos que pudiera cometer una persona empleada en esa entidad. Ahora, en cambio, hay que ir mucho más allá y proteger los intereses de la Unión Europea, que es algo que nos circunda a todos y que permite el tipo de vida que llevamos en este espacio privilegiado de la tierra. Ahora hay una exigencia externa y proveniente de la autoridad pública, para que se revisen los distintos canales que tienen las organizaciones y los relacionen entre sí para incrementar su eficacia. Para conseguir que cualquier tipo de infracción no se resuelva en un espacio restringido de la organización, sino que exista por encima una persona responsable que los analice y los combata de forma conjunta.

El salto de cómo es un canal de denuncias habitual a cómo debe ser el canal que ahora te exige la nueva ley, es un salto que las organizaciones más pequeñas deberán abordar con un mayor esfuerzo en cuanto a su rigurosidad y su sistematización. Sin embargo, este esfuerzo será aún más costoso, en cuanto a su integración con otros sistemas similares, para aquellas entidades más complejas y de mayor volumen que cuenten con filiales en diferentes países o con distintas sociedades en un mismo grupo empresarial.

Para el caso de las organizaciones más pequeñas y sencillas, bastará con tener un único canal de denuncias, que se integrará en el Sistema Interno de Información de esa organización. En el canal se gestionarán todas las informaciones que se reciban, y la gran diferencia con respecto a lo que exige la nueva ley, será que en el canal habrá que distinguir claramente entre los tipos de incumplimientos que se investiguen según sea la normativa específica que les afecte. Esto es, distinguiendo al menos entre infracciones penales y administrativas graves o muy graves, acoso laboral y sexual, blanqueo, terrorismo y ética.

Como acaban de ver, entre los tipos de informaciones a investigar por un canal, hemos incluido aposta la ética. La ética no es una

exigencia legal, pero sí es crucial para el éxito de lograr una cultura de cumplimiento dentro de las organizaciones. Así lo señala expresamente la referida Circular 1/2016 de la Fiscalía General del Estado, pero también lo señalan las teorías al respecto y el propio convencimiento que tienen las organizaciones sin ánimo de lucro según sus propias publicaciones. La norma específica que regula lo qué es ético o no, debería ser el código ético o de conducta que la propia organización elabore y apruebe siguiendo los estándares más exigentes de su sector.

En cuanto al caso de las organizaciones más grandes, la nueva ley complica su aplicación puesto que los canales que existan en su interior deberán acabar ligados y obligados entre sí bajo la autoridad y seguimiento de un único responsable del sistema interno de información. Este responsable del sistema puede ser una sola persona física o un órgano colegiado y, en todos los casos, cada canal que tenga la organización le deberá rendir cuentas internamente cada año sobre los resultados que haya obtenido. No obstante, se procurará que cada canal informe de manera agregada y relacionada, respetando en cada caso el nivel de confidencialidad correspondiente. Resumiendo, en una organización puede haber una persona responsable por cada canal, pero siempre habrá un responsable de todo el sistema interno de información. Si además se elige la opción de que el responsable del sistema sea colegiado, podría tratarse de un grupo donde estén los responsables de cada canal. Asimismo, la entrada a cada uno de esos canales deberá ser muy sencilla e inequívoca, por lo que se recomienda que exista un único acceso a esos canales. Ese acceso deberá permitir a la persona informante elegir el canal de forma sencilla, según el tipo de denuncia que quiera presentar o la entidad dentro del grupo sobre la que quiera informar. O, en el caso de que el informante tenga dudas del canal al que debe dirigir su información, ese acceso deberá asegurar que solo exista una persona responsable (unipersonal o colegiado; interno, externo o mixto) de gestionarlo y que sea esa persona quien derivará cada caso a la persona responsable del canal que corresponda. Sea cual sea la manera en la que se disponga ese acceso, es necesario insistir en que una organización podrá tener varios canales diferentes, pero siempre un único sistema interno de información que tendrá su propio responsable.

Asimismo, el sistema interno y el canal/es que esté/n integrado/s en ese sistema, formarán parte a su vez del programa de cumplimiento de la organización. Como ya hemos señalado, éste no solo deberá actuar frente a la posibilidad de que haya ocurrido una infracción de distinta tipología, sino que también deberá someter a su organización a la evaluación periódica de sus riesgos y a la aprobación de medidas que corrijan, mitiguen o eviten esos riesgos. Algo relacionado no ya solo con el cumplimiento de leyes y normas, sino más con la pura gestión interna, los procesos, los objetivos y la mejora continua.

CAPÍTULO 2. PRINCIPIOS BÁSICOS PARA UN SISTEMA INTERNO DE INFORMACIÓN

Patricia Fernández
Técnica del área Económica y Financiera de Medicus Mundi

Desde la reciente aprobación (21 de febrero de 2023) de la Ley 2/2023 reguladora de la protección de las personas que informan sobre infracciones normativas y de lucha contra la corrupción, estos principios y criterios que vamos a desarrollar no son meras recomendaciones para las organizaciones, sino que se han traducido en criterios claves para crear confianza y proporcionar un elevado nivel de protección a aquellas personas que se decidan a informar sobre conductas y/o acciones que puedan ser constitutivas de infracciones penales, administrativas, así como de cualquier, indicio, sospecha o evidencia de comportamiento contrario al Código de Conducta o Ético de una organización, suponga un acto delictivo o no.

ESTOS PRINCIPIOS Y CRITERIOS SON:

- **Accesibilidad**[1]: este principio se traduce en que el canal de denuncias debe ser claro, ha de ser fácil de usar y permitir que cualquier persona, ya sea perteneciente a la organización o no, pueda tener acceso al mismo, para que así puedan comunicar una irregularidad de la que hayan sido testigo y/o sea conocedora.

  Toda la información referente a las comunicaciones, los procedimientos aplicables y sobre el personal responsable de tratar las mismas, debe ser transparente y fácilmente comprensible, con el objeto de promover las comunicaciones y no de obstaculizarlas.

  Lo ideal es que el canal de denuncias esté de manera visible en nuestra página web y por qué no, traducido a todas aquellas lenguas que consideremos necesarias. De igual manera, tenemos que conseguir que el canal de denuncias sea accesible a personas con capacidades diversas, tales como personas carentes de habilidades de lectura y escritura, discapacidad visual, auditiva, etc. y es fundamental que todas las personas sepan a quién tienen que dirigir una comunicación.

  Ejemplo: Para que el canal de denuncias pueda ser accesible a todas las personas, en el caso de organizaciones que estén presentes en zonas donde las personas beneficiarias no tienen acceso a internet, es recomendable valorar la posibilidad de tener una persona responsable en la zona que se encargue de dar formación a las personas beneficiarias sobre: cómo denunciar, qué cosas pueden ser susceptibles de denunciar, distribuir folletos informativos, así como recibir y gestionar las denuncias. La formación en estas situaciones es fundamental.

  Además, para conseguir una mayor accesibilidad se debe permitir la recepción de las comunicaciones no sólo a través de una plataforma tecnológica, sino también de manera verbal, por escrito, a través de correo postal, por vía telefónica, a través de un sistema de mensajería de voz, o a través de una reunión presencial.

- **Transparencia**[2]: consiste en la obligación que tiene la organización de definir y publicitar su canal de denuncias, especificando qué se puede comunicar, cómo se debe presentar y formalizar la comunicación, cómo se tramitará la comunicación y qué órgano será el encargo de cada parte del proceso de una manera clara, coherente y actualizada.

- **Seguridad**[3]: cabe resaltar que todos los datos personales que se generen en la gestión de una comunicación deberán estar sujetos a una serie de medidas de seguridad que establezca la organización. Por tanto, la organización deberá contar con un sistema interno de información que contemple medidas técnicas y organizativas (implantar mecanismos para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos que nos faciliten, así como procedimientos de seguridad) para preservar la confidencialidad y la limitación del acceso a esta información y que aseguren además la protección de los datos de carácter personal (ver más abajo el apartado específico de "Protección de Datos"). A nuestro juicio, un correo electrónico como sistema para recibir comunicaciones, no sería un canal de denuncias idóneo para garantizarla con-

[1] Artículo 25 de la Ley2/2023. Desarrollado en el Capítulo 2. Ámbito objetivo y subjetivo. Apartado: Ámbito subjetivo.

[2] Artículo 25 de la Ley2/2023.

[3] Artículo 5.2b de Ley2/2023.

fidencialidad, ya que puede ser hackeado y podrían acceder al mismo. No obstante, la confidencialidad también depende en gran medida de las personas que tengan acceso a las comunicaciones y/o de los procedimientos para evitar accesos no autorizados. De este modo, por muy sofisticada que sea una plataforma o herramienta de nada sirve si las personas que reciben esas comunicaciones no respetan el carácter confidencial de la misma o si no hay cierto control sobre los profesionales que tienen acceso a la información.

La confidencialidad, disponibilidad e integridad de la información son algunas de las propiedades básicas de la seguridad y además serán los parámetros que nos permitan clasificar la información para seleccionar las medidas de protección que debemos aplicar a cada tipo. Las medidas de seguridad que tengamos que poner en marcha dependerán del tipo de sistema que queramos proteger, de la información que contengan, de las amenazas a las que se expongan y por supuesto de los recursos económicos con los que contemos.

Es importante tener en cuenta que, si la información que consideramos crítica se viese alterada, se destruyera o resultara inaccesible, podría causar graves consecuencias a las organizaciones, de ahí que las medidas de seguridad a implantar deberán ser proporcionales al riesgo que queramos evitar.

En este apartado no vamos a establecer una serie de medidas de seguridad específicas relacionadas con el servidor, antivirus, copias de seguridad, firewalls, cifrado de datos, sistemas de anonimización, etc., ya que, como se ha mencionado, dependerá de muchos factores; por ello se recomienda acudir a las páginas webs del Instituto Nacional de Ciberseguridad de España (INCIBE) y/o a la Agencia Española de Protección de Datos (AEPD), que son 2 organismos que han trabajado sobradamente, elaborando guías, que nos pueden servir de gran ayuda para proteger nuestra información.

Hacer ''click'' para acceder a la página de AEDP

Hacer ''click'' para acceder a la página de INCIBE

- **Confidencialidad**[4]: este principio implica que la organización no podrá revelar la identidad de la persona informante y de cualquier otra tercera persona, que se mencione en la comunicación, así como de las actuaciones que se lleven a cabo en la propia gestión de esta. Esta información tendrá carácter confidencial y no podrá ser comunicada, sin su consentimiento, a ninguna persona que no sea el responsable del sistema interno de información o el personal competente para recibir y gestionar las comunicaciones, que quedará regulado en el procedimiento interno (y que deberá elaborar la organización), con la excepción de que podrá ser comunicada a la Autoridad Judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora. Pero en este caso la organización deberá comunicar por escrito a la persona informante los motivos de la revelación de sus datos. Dicha cesión de datos a las autoridades administrativas o judiciales se realizará siempre dando pleno cumplimiento a la legislación sobre protección de datos de carácter personal.

  En el caso de que una persona reciba una comunicación y ésta no sea la encargada de recibirlas, deberemos garantizar que el personal que la haya recibido no pueda revelar cualquier información que pudiera permitir identificar a la persona informante o a la persona afectada y deberá remitir lo más pronto posible la comunicación a la persona responsable del tratamiento, con el fin de garantizar la confidencialidad de los datos.

  Ejemplo:

  La organización garantiza que:

  - Se respetará la confidencialidad de la persona informante y de cualquier otra tercera que se mencione en la denuncia, durante todo el proceso que engloba la recepción, valoración e investigación de la misma.

  - Se asegurará la imposibilidad de rastreo de la información, mediante elementos tecnológicos.

  - Se evitará la divulgación no necesaria de la información.

[4] Artículo 5.2b de la Ley2/2023.

Recomendación: la organización podría preparar un acuerdo de confidencialidad para que, con anterioridad, fuese firmado por todas aquellas personas involucradas en el proceso.

- **Limitación de acceso a los datos**[5]: la organización deberá delimitar el acceso a los datos contenidos en la denuncia, de tal manera que se acotará el número de personas que integren el órgano colegiado, si le tenemos como responsable del sistema interno de información, al igual que haremos lo mismo con el equipo investigador y órgano decisorio, ya que es importante reducir al máximo posible la cantidad de personas que pueden acceder a esta información.

- **No represalias**[6]: la organización deberá garantizar que no tomará ninguna medida disciplinaria, ni acción legal contra la persona informante, siempre que la comunicación se haya realizado de buena fe.

  Por trato desfavorable podemos entender cualquier tipo de medida negativa y significativamente de amenaza, discriminación o acoso que sufra la persona informante por parte de una persona integrante de la organización. Esta acción será investigada y, en su caso, sancionada oportunamente y cuando pudieran ser constitutivas de delito, el órgano encargado lo pondrá en conocimiento de la autoridad competente.

  Debemos tener en cuenta que, en los procedimientos ante un órgano jurisdiccional u otra autoridad relativos a los perjuicios sufridos por las personas informantes, una vez que la misma haya demostrado que ha comunicado o ha hecho una revelación pública y que ha sufrido un perjuicio, se presumirá que el perjuicio se produjo como represalia por informar o por hacer una revelación pública. En esos casos, siempre corresponderá a la persona que haya tomado la medida perjudicial probar que esa medida se basó en motivos debidamente justificados, no vinculados a la comunicación o revelación pública.

  Algunos ejemplos de represalias[7]:

[5] Artículo 32 de la Ley2/2023.

[6] Artículo 5.2b de la Ley2/2023.

[7] Para ver el listado completo de represalias ver el artículo 36.3 de la Ley2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

biblioteca COMPLIANCE WORLD COMPLIANCE ASSOCIATION

- Cambio de puesto de trabajo, cambio de ubicación del lugar del puesto de trabajo, reducción salarial…
- Denegación de formaciones o cursos, denegación de licencias o permisos…
- Evaluación o referencias negativas sobre resultados laborales.
- Suspensión, despido o destitución…
- Imposición de medidas disciplinarias, como la disminución de periodos de descanso o vacaciones.
- Intimidaciones, acoso, discriminación o trato desfavorable.
- Difamaciones tanto dentro como fuera del entorno laboral.
- Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, exclusión, rechazo o ignorar a una persona.

Por otra parte, si la comunicación se demuestra que no ha sido de buena fe, la organización se reservará el derecho de imponer las sanciones disciplinarias y/o acciones judiciales pertinentes. Se entiende por represalia cualquier acto u omisión que esté prohibido por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, sólo por su condición de personas informantes.

- **Seguimiento diligente de las comunicaciones**[8]: la organización deberá nombrar personas formadas y competentes que participen en todo el proceso de gestión de las comunicaciones (aplicable tanto para las personas que se encargan de la recepción, como las que participen de la investigación y resolución de estas) debiendo poseer capacidad y autonomía suficiente, y debiendo ser imparciales en cada comunicación que se reciba. El procedimiento interno deberá recoger que plazos (cumpliendo con los estipulados en la ley o in-

[8] Artículo 9.1.e) DIRECTIVA (UE) 2019/1937 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.

cluso pudiendo ser más exigentes), y como debe de realizarse la investigación, garantizando en todo momento el seguimiento de las comunicaciones de manera rápida y eficaz.

- **Anonimato**[9]: la Ley 2/2023 reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, nos deja claro que las comunicaciones podrán realizarse de manera anónima. Por tanto, los canales de denuncias deberán estar preparados para permitir la presentación y posterior tramitación de comunicaciones anónimas, pudiendo recibir comunicaciones en las que no se identifica la persona informante.
  Garantizar este anonimato será esencial y fundamental para que las organizaciones reciban comunicaciones que de otra manera la persona informante no se atrevería a señalar, por temor a represalias, en caso de ser identificadas.

- **Imparcialidad**[10]: para garantizar la imparcialidad es fundamental que la organización deje claramente regulado, en el procedimiento de gestión interno, cómo se llevará a cabo la gestión de las comunicaciones recibidas, desde la recepción hasta la resolución, además de qué persona o personas van a formar parte en las diferentes fases de recepción, investigación y resolución y sin olvidar regular también qué haremos o cómo procederemos ante un conflicto de interés (como pudiera ser que una de las personas afectadas por una comunicación interpuesta fuese una persona miembro del órgano que recibe, que investiga y/o que resuelve el caso).

  - Con relación a las personas que intervienen por parte de la empresa en la recepción, investigación y resolución, debe tenerse en cuenta que, aunque la recepción e investigación puede materializarse en la misma persona o bien en personas diferentes, lo que sí es obligatorio que en las fases de investigación y resolución las personas no sean las mismas.

  - Por otra parte, hay organizaciones que para garantizar en mayor medida esta imparcialidad, deciden contar con personas externas u órganos asesores externos, que participan en la fase de recepción de las comunicaciones, debiendo en aquellos casos en que no cuenten con esa posibilidad, garantizar la imparcialidad durante todo el proceso de gestión de la comunicación.

    Ejemplo: las personas que participen en la recepción, valoración e investigación de las denuncias, podrían firmar una declaración responsable de ausencia de conflicto de interés y que, aun habiendo sido firmado, si en el transcurso de la investigación surge este conflicto, habrán de abstenerse de seguir en el proceso.

[9] Artículo 6 de la Ley2/2023.

[10] Artículo 6.2 y 8.5 de la Ley2/2023.

biblioteca COMPLIANCE WORLD COMPLIANCE ASSOCIATION

2.1 DERECHOS DE LA PERSONA INFORMANTE, DE LA PERSONA AFECTADA Y DE OTRAS TERCERAS PERSONAS

Aunque no existe una lista reglada de los derechos pertenecientes a cada uno de estos grupos de personas, a continuación se identifican una serie de derechos que pueden recogerse en el procedimiento de gestión interno, y que sin ser limitativos, las organizaciones deberían de reflexionar de manera interna, en función de las particularidades de las mismas.

Derechos de la persona informante:

- Derecho al anonimato, no revelando la identidad de la persona informante.
- Derecho a la confidencialidad de los datos, personales o no, tanto de la persona informante como de cualquier otra tercera que se mencionen durante la gestión de la comunicación.
- Derecho a la protección de los datos personales. La persona informante tendrá derecho a que se le informe de quien es el responsable del tratamiento, así como, de dónde se conservan sus datos, quién tiene acceso a ellos, durante cuánto tiempo se conservarán, así como el derecho de acceso, rectificación, oposición, supresión, olvido de los datos, limitación del tratamiento, portabilidad de los mismos…
- Derecho de no represalia, siempre que actúe de buena fe.
- Derecho a recibir un acuse de recibo por parte de la organización, para comunicarle la recepción de la comunicación, siempre en un plazo no superior a 7 días naturales desde su recepción, salvo puesta en peligro su confidencialidad.
- Derecho a que se la informe de manera pertinente sobre el funcionamiento del canal de denuncias.
- Derecho a tener una investigación rigurosa e imparcial.
- Derecho a ser informada de la resolución o archivo de la comunicación.
- Derecho al apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la Autoridad Independiente de Protección del Informante [11], tras la valoración de las circunstancias derivadas de la presentación de la comunicación.
- Derecho a la asistencia jurídica en los procesos penales y en los procesos civiles transfronterizos, de conformidad con la normativa comunitaria.
- Derecho a la asistencia efectiva por parte de las autoridades competentes ante cualquier autoridad pertinente implicada en su protección frente a represalias, incluida, la certificación de que pueden acogerse a protección.
- Derecho a que la identidad no sea revelada en caso de revelación pública[12], con excepción de que sea sólo comunicada a la autoridad judicial.

Adicionalmente, sin perjuicio de lo anterior, hay que destacar que los informantes, además de derechos, también tienen obligaciones como:

- Actuar de buena fe. Las denuncias de mala fe podrán dar lugar a las medidas disciplinarias y/o sancionadoras que en su caso procedan contra el denunciante.
- Aportar los datos y documentos de los que disponga relacionados con los hechos denunciados.
- Deber de confidencialidad. El denunciante no podrá comunicar a ningún órgano o persona distintos de la persona responsable de recibir las comunicaciones, la identidad del denunciado, con las excepciones legalmente previstas.

Derechos de la persona afectada:

- Derecho a la confidencialidad de los datos, personales o no, tanto de la persona afectada como de cualquier otra tercera que se mencionen durante la gestión de la comunicación.
- Derecho a la protección de los datos personales. La persona afectada tendrá derecho a que se le informe de quien es el responsable del tratamiento, así como, de dónde se conservan sus datos, quién tiene acceso a ellos, durante cuánto tiempo se conservarán, así como el derecho de acceso, rectificación, oposición, supresión, olvido de los datos, limitación del tratamiento, portabilidad de los mismos…
- Derecho a la presunción de inocencia.
- Derecho de acceso al expediente, sin revelar la identidad de la persona informante y la de otras personas afectadas por el expediente.
- Derecho a aportar aquellos me-

[11] Título III de la Ley 2/2023. La Autoridad Independiente de Protección del Informante, A.A.I., es una autoridad administrativa independiente, con personalidad jurídica propia, plena capacidad de actuar de manera pública como privada, con potestad administrativa, consultiva y sancionadora.

[12] Título V de la Ley2/2023.

dios de prueba que considere adecuados y pertinentes.

- Derecho de rectificación de los datos que sean incompletos o inexactos.
- Derecho de defensa. Tienen derecho a ser escuchadas, con el fin de argumentar en su defensa todo aquello que consideren oportuno.
- Derecho a no sufrir represalias adicionales a la posible sanción que pueda derivarse.
- Derecho a que se la informe de la resolución o archivo de la comunicación.
- Derecho a contar en todo momento con el asesoramiento de la representación legal de las personas trabajadoras, en el caso de haberlas, o de un/a abogado/a, a efectos de ejercer su defensa.

Derechos de la persona afectada:

- Derecho a la confidencialidad de los datos, personales o no, que se mencionen durante la gestión de la comunicación.
- Derecho a la protección de los datos personales. Tendrán derecho a que se les informe de quien es el responsable del tratamiento, así como, de dónde se conservan sus datos, quién tiene acceso a ellos, durante cuánto tiempo se conservarán, así como el derecho de acceso, rectificación, oposición, supresión, olvido, limitación del tratamiento, portabilidad de los mismos…

Aunque estos derechos la Ley 2/2023 sólo los acota para las personas que participen en la gestión de las comunicaciones, cuando los hechos denunciados estén contemplados en la misma, se recomienda que estos derechos se apliquen para cualquier comunicación o hecho denunciado. Así las cosas, el artículo 3.4 de la Ley 2/2023 establece que también tendrán derecho de protección:

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

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

c) Las personas jurídicas, para las que trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa. A estos efectos, se entiende que la participación en el capital o en los derechos de voto correspondientes a acciones o participaciones es significativa cuando, por su proporción, permite a la persona que la posea tener capacidad de influencia en la persona jurídica participada.

2.2 PROTECCIÓN DE DATOS PERSONALES[13]

Los tratamientos de datos personales se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Las organizaciones no deben olvidar que al iniciar el procedimiento de gestión de una comunicación se va a producir un tratamiento de datos personales y por supuesto será necesario requerir el consentimiento expreso de la persona informante, para la inclusión y tratamiento de sus datos personales teniendo limitada la posibilidad de comunicación de dicha identidad sólo a la autoridad judicial, al Ministerio Fiscal o la autoridad administrativa competente, exigiendo que en todo caso se impida el acceso por terceras personas a la misma. Por tanto, sólo se puede tratar los datos personales sin el consentimiento expreso de la persona informante, siempre y cuando sea en cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos otorgados a la persona responsable del tratamiento.

La persona informante garantizará que los datos personales proporcionados son verdaderos, exactos, completos y actualizados y se compromete a comunicar a la organización cualquier modi-

[13] Título VI de la Ley 2/2023.

ficación de los mismos. Además, la persona informante que haga uso del canal de denuncias tendrá que aceptar de manera plena y sin reserva la política de privacidad que tenga la organización.

No se debe recopilar aquellos datos personales que no sean necesarios para abrir una investigación o, si se recopilaran por accidente, existiría la obligación de eliminarlos. Además, en caso de que la información facilitada por la persona informante no sea veraz, se debe eliminar, salvo que esta falta de veracidad pueda constituir un ilícito penal, en este caso, de guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

Eso sí, transcurridos 3 meses desde la recepción de la comunicación sin que se haya iniciado una investigación, se debe proceder a la eliminación de la información, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema, en cuyo caso sólo podrán constar de forma anonimizada, sin que sea necesario en ese caso bloquear la información.

Los datos que finalmente sean objeto de tratamiento podrán conservarse sólo durante el tiempo imprescindible para decidir si iniciamos una investigación[14].

La Ley 2/2023 establece qué personas podrán tratar los datos de carácter personal:

- La persona responsable del sistema, que podrá ser el órgano de gobierno de la organización, una persona física o un órgano colegiado e incluso una persona tercera a la que se le haya delegado esta función.
- Las personas que participen en la gestión de la comunicación, desde su recepción hasta la resolución.
- La persona responsable de recursos humanos o el órgano competente designado para ello, sólo en el caso de que se diera lugar a la adopción de medidas disciplinarias contra una persona trabajadora.
- La persona responsable de los servicios jurídicos de la organización, siempre que se proceda a la adopción de medidas legales en relación con los hechos relatados en la comunicación.
- Las personas encargadas del tratamiento que eventualmente se designen.
- La persona delegada de protección de datos, si la hubiera.

Podrán tratar los datos otras personas distintas a estas, o incluso se podrá hacer una comunicación a otras terceras personas, cuando resulte necesario para la adopción de medidas correctoras en la organización o para la tramitación de procedimientos sancionadores o penales.

Ejemplo de política de privacidad disponible en el canal de denuncias y accesible para las personas que hagan uso del canal de denuncias:

Persona responsable del tratamiento de tus datos: la entidad responsable del tratamiento de la información obtenida de las comunicaciones y de las investigaciones es XXXXX (C.I.F. XXXXX, Calle XXX, Número XX, Código Postal XXXX, Localidad XXXX Provincia XXXXX) o en su caso, los datos de contacto de la persona delegada de protección de datos.

Tratamiento de los datos: los datos obtenidos de las comunicaciones o de las investigaciones realizadas por el canal de denuncias serán tratados para la investigación de los hechos denunciados y para la prevención de la posible comisión de infracciones.

Comunicación de los datos: de forma general, sólo tendrá acceso a esta información, en primera instancia, la entidad XXXXXXXX. Dicha información podrá ser comunicada a otras terceras personas cuando sea necesario para el buen fin de la investigación, en cualquiera de sus fases, cuando una ley así lo prevea o con el previo consentimiento de las personas afectadas.

Base jurídica de los tratamientos: la base para el tratamiento de los datos es el interés legítimo en prevenir, investigar y controlar cualquier comportamiento irregular, ilícito o delictivo producido en el seno de la organización, así como el cumplimiento de la obligación legal de gestionar las denuncias según establece la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Cuánto tiempo conservaremos los datos: Los datos que son objeto de tratamiento en el marco de las investigaciones serán cancelados tan pronto como éstas hayan finalizado. En ningún caso podrán conservarse los datos por un período superior a diez años.

[14] Artículo 26.2 de la Ley 2/2023. Los datos personales relativos a las informaciones recibidas y a las investigaciones internas realizadas no podrán conservarse por un período superior a diez años

Cuáles son tus derechos: Tiene derecho a obtener confirmación de si estamos tratando o no sus datos personales y, en tal caso, acceder a los mismos. Puede igualmente pedir que sus datos sean rectificados cuando sean inexactos o a que se completen los datos que sean incompletos, así como solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos, mediante comunicación escrita dirigida a XXXXX o a través del correo electrónico XXXXXXXX, o bien pudiendo hacer uso de los modelos que pone a disposición de la ciudadanía la Agencia Española de Protección de Datos en su Web.

En determinadas circunstancias, podrá solicitar la limitación del tratamiento de sus datos. En tal caso, sólo se tratarán los datos afectados para la formulación, el ejercicio o la defensa de reclamaciones o con miras a la protección de los derechos de otras personas.

En determinadas condiciones y por motivos relacionados con su situación particular, podrá igualmente oponerse al tratamiento de sus datos. En este caso, se dejarán de tratar los datos salvo por motivos legítimos imperiosos que prevalezcan sobre sus intereses o derechos y libertades, o para la formulación, el ejercicio o la defensa de reclamaciones.

Puede revocar el consentimiento que hubiese prestado para determinadas finalidades, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

biblioteca COMPLIANCE WORLD COMPLIANCE ASSOCIATION

CAPÍTULO 3: ÁMBITO OBJETIVO Y SUBJETIVO

Guillermo González de la Torre Rodríguez
Coordinador de Estrategia y Calidad de Manos Unidas

Del análisis realizado por las organizaciones autoras de esta publicación, queda de manifiesto que el alcance que debería tener un canal de denuncias y un sistema interno de información debería ser tal que cualquier persona pueda informar de cualquier hecho reprobable relacionado con una organización y que lo haga de forma protegida. El alcance del canal en ese sentido debería ser total. Como se desarrolla a continuación, esta sería la única forma de preservar la integridad y la ejemplaridad con la que deben comportarse las organizaciones del sector sin ánimo de lucro.

Es verdad que, en puridad, las leyes relacionadas con el tema (ver capítulo 1 sobre "Introducción") no obligan a que se haga de este modo. Si se analizan de forma estricta esas leyes, se podría establecer un conjunto de instrucciones que primero distinga cuáles son las categorías de denuncias que se podrían admitir o no en un canal de denuncias. Es decir, que más allá de los criterios de admisión, archivo y clasificación que se explican en esta guía, podría negarse a abordar cualquier información que no encaje con los temas exactos que recogen esas leyes. Y, a continuación, según sean esas categorías, también se podría definir qué medidas de protección y garantías se pueden adoptar con las personas que se vean implicadas en ellas, siguiendo literalmente los requisitos de esas leyes. Es decir, se aplicaría distintos niveles de mayor o menor consideración y protección según fueran los hechos, las faltas y las personas informantes que se gestionen en ese canal.

Teniendo en cuenta lo anterior, se considera que, estas distinciones tan rigurosas, no serían coherentes con los valores que tienen las entidades sin ánimo de lucro, las cuales surgen en general como inquietud solidaria y reivindicativa de un grupo de personas que promueven el interés general y luchan por los derechos de otras personas más vulnerables. Valores por los que no discriminamos nunca a nadie por ninguna condición, sea etnia, género, religión, lengua, ideología o cultura. Y mucho menos no se debe rechazar a una persona informante por cuál

es su relación con la organización, por cuál es su preparación y capacidad, o por cuál es la adecuación exacta de lo que presenta en el canal con respecto a un requisito legal muy concreto que puede no comprender o tener en cuenta en un primer momento.

Tanto son así estos valores, que las referencias más fundamentales del sector suelen apelar a esta dimensión ética como compromiso ineludible de dichas entidades para actuar en la sociedad. Como ejemplos, podemos citar las características y los conceptos básicos del código de conducta de La Coordinadora de Organizaciones para el Desarrollo de España, las recomendaciones éticas del Tercer Sector de Acción Social o los principios del código de conducta y buen gobierno de la Asociación Española de Fundaciones. Pero hay más, muchas más referencias y ejemplos.

Asimismo, existe mucha conciencia sobre la responsabilidad en los fondos económicos que se gestionan y sobre el impacto social que genera las actividades desarrolladas por las entidades no lucrativas. Dichas entidades se encuentran altamente exigidas frente al escrutinio público y dependen enteramente de la confianza de la sociedad para existir y acometer sus fines. Es por eso, que es necesario extremar siempre la precaución a la hora de emplear los recursos.

El nivel de complejidad que requiere operar en este sector, repleto de exigencias legales, normativas y sectoriales de todo tipo, hace obligatorio adoptar los más altos estándares y prácticas de calidad y profesionalidad, lo cual lleva a especializarse en temas muy específicos y complejos como la fiscalidad, la planificación, la sostenibilidad, el medio ambiente, el género, la calidad, la prevención de delitos, la digitalización, los riesgos laborales o la seguridad, entre otros.

Por todos estos motivos, es fundamental hallar siempre el equilibrio entre el gasto sensato y austero encaminado a los fines sociales, y la necesidad de abordar iniciativas de gestión de gran envergadura y nivel técnico. En esto último encajaría la implementación de un sistema interno de información que integre todos los canales de denuncias, en caso de que la organización cuente con más de uno, y la manera de vincularlo con el sistema de cumplimiento normativo que haya implantado.

biblioteca COMPLIANCE WORLD COMPLIANCE ASSOCIATION

Que decir que este equilibrio resulta aún más difícil de alcanzar cuando se trata de organizaciones pequeñas y con pocos recursos. En esos casos, existe una opción a valorar como es la de contratar y compartir entre varias organizaciones de fines y valores similares, una entidad externa e independiente que dé servicios a los canales específicos de esas organizaciones a través de una plataforma online común.

En cualquier caso, para las entidades sin ánimo de lucro, la ética no se negocia, y esta premisa, debe acompañarnos en cada paso que se de y en cada decisión que se tome. De este modo, sea cual sea la circunstancia de una organización, el alcance del canal de denuncias debería ser siempre total, este alcance se debe cumplir tanto en el ámbito objetivo (qué se puede denunciar, comunicar o informar), como en el ámbito subjetivo (quién lo puede hacer).

3.1 ÁMBITO OBJETIVO:

Desde el ámbito objetivo, el canal de denuncias de una organización debería permitir que se pueda recibir cualquier tipo de información que una persona informante considere de interés, aunque no toda esa información será atendida por el canal para su posterior investigación si no se ajusta a su objeto. Es decir, no debe existir en ese canal ningún requisito de concretar la información de un modo tal que impida presentar una denuncia por no cumplir con ese requisito. Pero, al mismo tiempo, ese canal debe tener unas reglas muy claras de funcionamiento que permitan analizar con criterios objetivos las denuncias que reciba, y rechazarlas o gestionarlas luego de forma específica según sean esos criterios. Por ejemplo, las denuncias de acoso sexual, cuya ley obliga a la persona informante a comunicar la identidad de las personas que estén implicadas y a concretar los hechos que se denuncian.

¿Cómo se compatibilizan, entonces, estas dos realidades en apariencia antagónicas? Ya que primero parece que podemos denunciar cualquier cosa, pero luego parece que la organización nos exigiera una forma determinada de presentar algunas denuncias, puesto que la organización realiza un análisis o la valoración preliminar a cada denuncia. Esta valoración, que también puede recibir el nombre de “test de admisibilidad”, determinará si la información recibida se ajusta a los términos

previstos por la organización para definir lo que es una denuncia, en cuyo caso la admitirá o no para su tramitación.

Es muy importante, además, diferenciar claramente una denuncia de otras informaciones que no lo son como las consultas, quejas y sugerencias. Si en esa valoración preliminar se detecta que la información encaja en esas otras tipologías, entonces la persona gestora del canal de denuncias deberá remitir esa información al canal o comité o departamento que se responsabilice en la organización de atender las consultas, las quejas o las sugerencias.

Se recomienda, a este respecto, que la organización tenga una definición clara y completa de lo que ella considera que es una denuncia, como de lo que considera que es una queja, una consulta o una sugerencia. Estas definiciones deberán estar colocadas en lugares visibles y de fácil acceso, así como se difundirán activamente. Servirán asimismo como criterios objetivos en la valoración preliminar para rechazar esa información al no ajustarse a término de lo que se considera una denuncia. Por otro lado, las quejas, consultas y sugerencias se deberán recibir y gestionar por un espacio o canal distinto y claramente diferenciado del canal de denuncias. De este modo, se habrá de desligar de la misma con procedimientos, objetivos, personas responsables y recursos bien diferenciados. Y si a este otro espacio de contacto llegara algo referido a una denuncia, bien por error o bien por uso incorrecto, la persona responsable de ese espacio deberá remitirlo de inmediato al canal de denuncias de la organización, aunque las exigencias de la Ley 2/2023 sólo se aplicarían al canal de denuncias, ya que el otro sería meramente informativo de temas que no atentan contra ninguna norma.

Con la valoración preliminar, por tanto, descargamos de toda exigencia previa a la persona informante a la hora de presentar su denuncia, para que así el canal no sea una barrera que impida que esa información se pierda. Será siempre suficiente con que la persona sienta o crea que está ante un hecho reprobable y que por ello se vea en la obligación de hacerlo saber para su investigación, tal como señalamos en la introducción de esta guía.

Eso sí, más allá de la variedad inmensa de situaciones que puedan darse según el perfil de las personas informantes, esto no es óbice para que esperemos y exijamos de algún modo un mínimo de corresponsabilidad en el uso del canal de denuncias. Es decir, que al mismo tiempo que una organización va más allá de sus obligaciones legales por un sentido amplio de la responsabilidad, del mismo modo debemos informar, apoyar, difundir, formar y sensibilizar para que las personas que empleen el canal también sean conscientes de su responsabilidad tanto para hacer buen uso del canal, como para conocer bien cómo funciona y así lograr que sus denuncias prosperen con mayor éxito.

En cualquier caso, insistimos en que no deberíamos pedirle a la persona informante que, aparte de dar ese paso difícil y necesario, encima tenga que preparar su denuncia con todo detalle y precisión, ya que ello supondría que tuviera que ser experta en el tema en cuestión, y que además la denuncia la tuviera que documentar y fundamentar al completo con pruebas y evidencias. Si ese fuera el caso, estaríamos entonces esperando a que la persona informante no solo informe, sino que también sea policía, detective y abogada. Algo que, por supuesto, escapa de su alcance y amenazaría la posibilidad de que el canal se use y de que la organización recibiera denuncias.

Es conveniente, en ese sentido, distinguir entre el hecho de que una persona informante puede denunciar sobre cualquier ámbito o cuestión, y entre el hecho distinto que supone el grado de detalle o precisión que se debería requerir o no en la presentación primera de esa denuncia. Este segundo aspecto, en muchas ocasiones, se va mejorando y alcanzando en posteriores interacciones cuando, a partir de su admisión a trámite, a la persona informante se le va exigiendo más explicaciones y evidencias a lo largo de la investigación.

La competencia de analizar cada denuncia para aclarar cuál es su categoría y cuáles son los hechos concretos que describe, debería ser de la organización. Y si los datos que se aportan no fueran suficientes, en un primer momento, para demostrar que el indicio de una conducta reprobable es razonable, la denuncia no se debería rechazar, sino que se debería admitir, abrir el proceso de investigación y contactar con la persona informante, si fuera posible, para que concrete y amplíe esta información.

Una vez que una organización tiene conocimiento sobre cualquier presunto delito o irregularidad, ésta ya no puede ignorar su obligación de tramitarlo, por mucho que luego pueda no demostrarse que ocurrió o pueda quedar inconcluso. Aunque en cada entidad residirá la libertad y la soberanía de decidir hasta dónde llegar para admitir a trámite una denuncia o para finalizar un proceso de investigación, matiz que deberá recoger con claridad en sus normativas propias.

En la valoración preliminar, el personal encargado deberá tener una formación o experiencia acreditada al respecto, así como unos criterios y unos procedimientos que indiquen la forma de proceder, según sean las denuncias que se reciban[1]. Pero, en cualquier caso, esos procedimientos deberán ser elaborados siguiendo la dimensión ética a la que aludimos al inicio. De tal manera, que se asegure que habrá siempre un interés previo de la organización por aprovechar cualquier denuncia en beneficio de la ley y del bien común, aunque eso suponga algún riesgo o daño para una parte de dicha organización.

En definitiva, siempre que se perciba que pueda existir un indicio, el canal de denuncias y las personas que lo gestionan, deberán ser un instrumento útil y eficaz para que la información sea coherente. Esta ayuda puede prestarse bien en la propia presentación y valoración preliminar, perfilando mejor su denuncia mediante la cumplimentación de unos campos mínimos, obligatorios e imprescindibles para su tramitación posterior; o bien, la organización podría prestar alguna medida de apoyo a las partes implicadas en la denuncia durante el proceso de investigación o instrucción, una vez que ya fue admitida a trámite, en las distintas comparecencias y solicitudes de información que se activan a lo largo del mismo.

Si la persona informante tiene alguna dificultad de comprensión o tiene miedo o es muy vulnerable ante los hechos que remite, esa ayuda se hará aún más evidente y se la podrá acompañar con mayor dedicación, si fuese necesario. De ahí la importancia de que los canales de denuncias permitan que se interpongan las denuncias no sólo de forma escrita, sino también mediante solicitud de reunión presencial y/o verbal, tal como estipula el artículo 7.2 de la Ley 2/2023. Sólo si la persona informante no da más información porque no quiere o porque eligió la opción del anonimato y no se pudiera contactar con ella, entonces la denuncia podría rechazarse en la misma valoración preliminar, si se diera el caso de que la información no fuera suficiente o no se ajustara a término. Y si se admitiera a trámite, pero luego en el proceso de instrucción se advirtiera que la información aportada no es suficiente para demostrar la acusación vertida en la denuncia, también se podría descartar la misma, pero se haría tras finalizar la investigación reglada correspondiente, en cuyo informe se recomendaría cerrar el caso por no encontrar resultados concluyentes.

Como se ve, el alcance total para el ámbito objetivo de un canal, tiene luego su propio proceso que permitirá a la organización analizar la denuncia según unos criterios y pasos determinados, tanto para ayudar a la persona informante y no desperdiciar ninguna oportunidad de lograr información relevante y atender a nuestro deber de socorro, como para dilucidar si esa información tiene base y pertinencia, para así rechazarla cuando se perciba que no la tiene y proteger de este modo los intereses de la organización frente a la confusión, el desconocimiento o la posible mala fe de una persona informante.

3.2 ÁMBITO SUBJETIVO:

Desde el ámbito subjetivo, el canal de denuncias de una organización debería permitir que cualquier persona externa o interna a la organización pueda remitir una denuncia, siendo relevante que el canal sea accesible a todas ellas. Es decir, que el canal debe permitir al menos dos aspectos esenciales:

1. Que no exista en ese canal ningún requisito que obligue a identificarse a esa persona o a exponer una condición de su identidad, puesto que, en caso contrario, se estaría incumpliendo la propia Ley 2/2023 (artículo 7.3).
2. Que no obligue tampoco a disponer de una capacidad física o intelectual determinada para poder hacer uso de ese canal.

Con el primer aspecto sobre identificación, nos referimos a algo que ya se menciona en esta publicación, y que es la posibilidad de que una persona pueda elegir entre el anonimato y la confidencialidad. Es algo que exige la ley española, trasponiendo lo que exige la directiva europea correspondiente, y es a su vez uno de los principios que fundamentan las motivaciones y

[1] Ver capítulo 4 de esta guía sobre "Fases en la gestión de denuncias en una organización".

objetivos de esas normas. Pero también nos referimos a que la opción de confidencialidad sea tratada con debida diligencia, para que la identidad de esa persona no sea revelada a nadie, fuera de las personas que son competentes en la materia dentro del sistema interno de información, y para que esa persona sea protegida contra cualquier represalia o daño que pueda sufrir, por el hecho en sí de haber denunciado. En caso contrario, también se estaría incumpliendo la Ley 2/2023 (artículo 31).

También es importante señalar en este aspecto que, para elegir la opción de confidencialidad, la organización podrá pedir algunos datos para identificar a la persona que denuncia. Pero esos datos nunca podrán ser excesivos, ni discriminatorios. Tendrán que ser los datos imprescindibles y necesarios para gestionar las denuncias, y así además deberá indicarse expresamente en el procedimiento interno de aquellas personas que se responsabilizan del sistema. Esto es, bastará con que se conozca su nombre, apellidos y vía de contacto, bien el email y/o el número de teléfono, y su vinculación con la organización.

Si la persona informante, a lo largo del proceso de denuncia, diera datos personales sensibles protegidos por la ley o aquellos que no sean estrictamente necesarios para el tratamiento de la denuncia, como la orientación sexual, el lugar de nacimiento, la religión o la situación económica, la organización deberá prestar especial cuidado en su tratamiento, acceso, archivo y eliminación.

En cuanto al segundo aspecto que un canal debe permitir referido a disponer o no de una capacidad determinada, tenemos también que un canal de denuncias deberá estar acondicionado para ser usado por todo tipo de personas con situaciones y capacidades diferentes. Esto es, el canal deberá permitir un acceso universal y, para ello, deberán existir múltiples opciones que respondan a toda esa diversidad y permita a cualquier persona abordar la tarea de presentar una denuncia:

- Personas carentes de habilidades de lectura y escritura o que no tengan internet: interlocutores o puntos focales.
- Personas con discapacidad visual, auditiva o con discapacidad del habla: lectura leída, audios, subtítulos, textos.
- Personas con comprensión disminuida: lectura fácil, botón de ayuda.
- Personas de otros países: versiones en distintos idiomas, traducción automática.

Por último, es conveniente destacar que la obligación de la organización de ayudar a la persona que informa no exime de la responsabilidad de esa persona ante la denuncia que presenta. En ese sentido, si esa persona no logra recabar información suficiente, o no consigue concretar y demostrar su acusación, la organización no podrá sustituirla en ese deber que es solo de esa persona. En esos casos, el comité de instrucción / equipo investigador deberá terminar la investigación con los recursos que se hayan podido obtener y planteará la recomendación que estime oportuna, por mucho que ésta pueda estar limitada o condicionada por esa falta de información.

En ese sentido, es importante que las organizaciones faciliten a las personas cómo denunciar y, en cualquier caso, que denuncien. Por eso es muy importante que las normas más relevantes de la organización sean conocidas y de fácil acceso, y que la referida al funcionamiento del canal se encuentre en el mismo apartado o lugar donde esté ese canal.

De todas maneras, cuando la persona que denuncia se encuentre ante una situación de riesgo, por estar sufriendo algún daño cierto o por poderlo sufrir en un futuro inminente, se le deberá prestar especial cuidado y brindarle la ayuda que sea posible. Como ya dijimos, para presentar una denuncia no puede haber más requisito que la voluntad de una persona de hacerlo por sentir o creer que está ante un hecho reprobable. Pero su responsabilidad ante la denuncia que presenta no deja nunca de existir.

Esta responsabilidad es aún más exigible si cabe cuando esa persona ni siquiera está en una situación de riesgo real. De hecho, se dan casos en los que una denuncia se trata en verdad de una percepción subjetiva sin fundamento de la persona informante, así como sesgada, distorsionada o condicionada por factores y por intereses personales, que nada tienen que ver con hechos que vulneran una norma dada y que, por lo tanto, sean ilícitos. Cabe recordar, además, que estos casos de denuncias de mala fe son delitos y, por tanto, sancionables, por lo que se debe promover siempre el uso responsable del canal.

En resumidas cuentas, en una denuncia siempre habrá que atenerse a si los hechos o las conductas denunciadas han podido ocurrir realmente, y a la norma concreta que se habría vulnerado o incumplido con esos hechos. Si esta ligazón no se demuestra ni se da, debemos averiguar si hubo mala fe o intención de mentir para hacer algún tipo de daño o para obtener algún tipo de beneficio. Si no fuera el caso, entonces podríamos estar ante dos situaciones distintas: que faltan recursos para probar la veracidad de lo que señala la persona informante; o que más allá de que se demuestren como veraces esos hechos, se valore que no constituyen falta contra ninguna norma, ya se propia o legal y, por lo tanto, no sea una denuncia en sí.

Si esa información no constituye falta contra ninguna norma, pero los hechos descritos en ella se consideran relevantes, la organización deberá atenderla para saber su importancia y así decidir si lo ignora o si lo gestiona. Tal como ya señalamos antes en el apartado de ámbito objetivo, estas informaciones son, por lo general, una queja, una consulta o una sugerencia. Pero, en todo caso, la configuración de acceso universal del canal deberá permitir siempre que la persona no desista en presentar su denuncia por tener alguna duda razonable sobre cómo hacerlo.

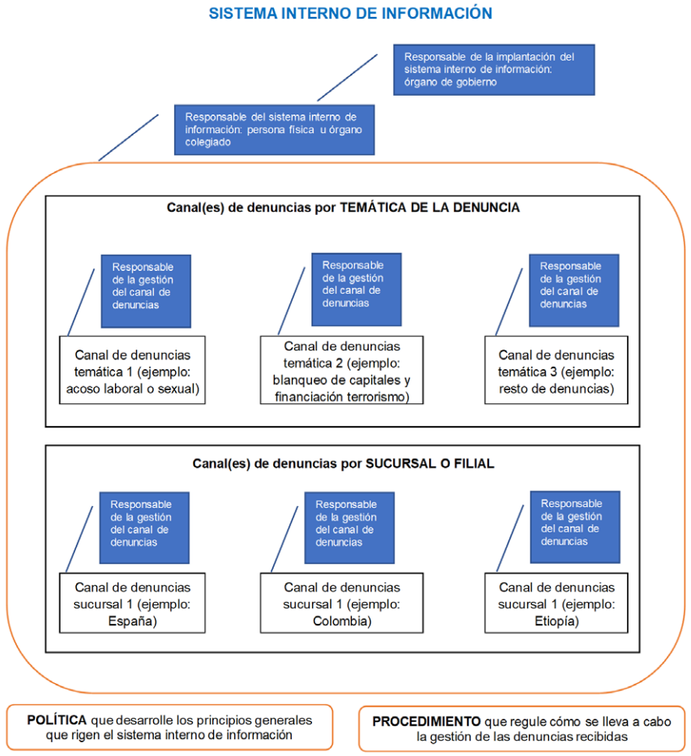
biblioteca COMPLIANCE WORLD COMPLIANCE ASSOCIATION

CAPÍTULO 4. FASES EN LA GESTIÓN DE DENUNCIAS EN UNA ORGANIZACIÓN

Laura Gonzalvo Diloy

Directora de Auditoría Interna y Control de Riesgos de la FIIAPP

Para que una persona comunique una denuncia deberá hacer uso del/de los canal(es) de denuncia(s) habilitado(s) por la organización, que estará(n) integrado(s) dentro del **sistema interno de información** de la organización. Dicho sistema deberá integrar todos los canales con los que cuente la organización para interponer denuncias. En caso de disponer de varios según la temática (por ejemplo, aquellas organizaciones que disponen de canales de denuncia para informar sobre posibles casos de acoso laboral y/o sexual), deberán estar todos ellos regulados por la política que desarrolle los principios generales que rigen dicho sistema (desarrollados en el capítulo 2 "Principios básicos para un sistema interno de información" de la presente guía), y por el procedimiento que regule cómo se llevará a cabo la gestión de las denuncias recibidas, desde su recepción hasta su posible comunicación a la autoridad competente.



El órgano de administración o de gobierno de la organización será el responsable de la implantación del sistema interno de información, previa consulta informativa con la representación legal de las personas trabajadoras, en caso de haberla, y, por tanto, tendrá la condición de responsable del tratamiento de los datos personales[1]. El órgano de administración o de gobierno de la organización deberá designar a la persona física responsable de la gestión del sistema interno de información, así como de su destitución o cese, si procediese. Si la organización optase por que el responsable del sistema fuese un órgano colegiado, este deberá delegar en uno de sus miembros las facultades de gestión del sistema interno de información y de tramitación de expedientes de investigación. La designación del responsable del sistema deberá reflejarse en acta del órgano de administración o de gobierno de la organización.

A continuación, se detallan cada una de las **actividades o fases que integran el proceso de gestión de las denuncias** dentro de una organización, así como directrices generales, que deberán adaptarse a las necesidades y contexto de cada organización, para su debido desarrollo:

4.1 COMUNICACIÓN DE LAS DENUNCIAS:

Para fomentar un uso adecuado y responsable del/de los canal(es) de denuncia(s), la organización deberá proporcionar la información de forma clara y fácilmente accesible, sobre el uso de dicho(s) canal(es), así como sobre los principios esenciales de su política (desarrollados en el capítulo 2 "Principios básicos para un sistema interno de información" de la presente guía), y aspectos más relevantes del procedimiento de gestión de las denuncias recibidas. En caso de contar con una página web, dicha información deberá constar en la página de inicio, en una sección separada y fácilmente identificable[2].

El canal de denuncias deberá permitir recibir comunicaciones por escrito, verbalmente o de ambas formas[3]:

- En caso de que la comunicación sea por escrito se podrá disponer de un formulario, online y/o descargable, o en su defecto determinar en el procedimiento qué campos son requeridos para presentar debidamente la denuncia, que podrían ser:

  - Razón de vinculación con la organización (persona contratada o voluntaria, persona miembro del órgano de gobierno, proveedor, persona beneficiaria, donante, etc.): este campo podrá ser opcional, pero es recomendable, ya que arrojará a la organización información interesante sobre el origen de las posibles irregularidades.

  - Nombre y apellidos: este campo deberá ser opcional, ya que la organización tiene la obligación de permitir denuncias anónimas, siendo decisión de la persona informante si desea identificarse o no.

  - Domicilio, correo electrónico y/o lugar seguro a efectos de recibir las notificaciones que se deriven del proceso: estos campos serán opcionales. Si la organización no cuenta con un canal que permita la comunicación bidireccional, es preciso aclarar que en caso de no disponer de esta información resultará inviable cualquier comunicación posterior con la persona informante.

  - Descripción de los hechos: este campo será obligatorio, dejando claro la necesidad de que se incluya información lo más precisa posible de la irregularidad, detallando fecha, lugar, personas implicadas y posibles personas testigos, así como adjuntar datos que sean pertinentes para su análisis preliminar posterior.

- En caso de que la comunicación sea verbal, a través de una reunión presencial (a mantener dentro del plazo máximo de siete días naturales desde su solicitud), telefónicamente o mediante sistema de mensajería de voz, deberán documentarse de alguna de las siguientes maneras:

  - Mediante una grabación de la conversación[4], en un formato seguro, duradero y accesible, debiendo permanecer dicha grabación debidamente custodiada y solo accesible a personal autorizado. Para la grabación, se deberá recabar previamente, el consentimiento de la persona informante de la grabación de la comunicación y, por tanto, al tratamiento de sus datos personales de acuerdo con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. A continuación, se incluye una propues-

[1] Artículo 5.1 Ley 2/2023.
[2] Artículo 25 de la Ley 2/2023.
[3] Artículo 7.2 de la Ley 2/2023.
[4] No es la práctica más recomendada, pero ante la falta de recursos, podría hacerse uso de los audios en el móvil, siempre y cuando, posteriormente,a la grabación se custodie adecuadamente.

ta de texto a leer a la persona informante, de forma previa a comunicar la denuncia:

Le informamos que esta conversación será grabada, de acuerdo con lo estipulado en el artículo 7.2 de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.
(Nombre de la organización), como responsable del tratamiento de sus datos personales, los tratará para gestionar debidamente las denuncias recibidas, y, por tanto, cumplir con las obligaciones legales a las que está sujeta.

Si desea conocer más sobre nuestra Política de Privacidad, la podrá consultar de forma íntegra en nuestra Web.

En base a lo anterior, ¿consiente la grabación de la conversación y, por tanto, el tratamiento de sus datos personales? DIGA SÍ O NO.

- A través de una transcripción completa y exacta de la conversación realizada por la persona responsable de la gestión del canal de denuncias.

En cualquier caso, se ofrecerá a la persona informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación, debiendo hacer constar también la firma de la persona responsable de la gestión del canal de denuncias.

Independientemente de cuál sea el canal interno de información a través del cual se formalice la denuncia, no se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratarla, o, si se recopilan por accidente, se eliminarán sin dilación indebida[5]. En cualquier caso, si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos[6], se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento[7].

Además, a quienes realicen la comunicación se les informará, de forma clara y accesible, sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea[8].

Cuando la denuncia sea remitida por canales que no sean los establecidos o recibida por miembros del personal no responsable de su gestión, se deberá poner en conocimiento de forma inmediata al responsable del sistema interno de información o a la persona responsable de la gestión del canal de denuncias, siendo ésta última quien procederá a su registro a través del canal correspondiente para así darle el debido trámite. Por tanto, no se podrá gestionar ninguna denuncia que no esté debidamente registrada en el canal de denuncias correspondiente.

En el momento en el que se comunica la denuncia, siempre y cuando no sea de forma verbal o no se realice de forma anónima y no se disponga de los datos de contacto del informante, se deberá emitir un acuse de recibo a la persona informante, en un plazo máximo de siete días naturales desde la recepción o registro de la denuncia, salvo que ello pueda poner en peligro la confidencialidad de la comunicación . En caso de disponer de un software, éste suele proporcionar un código de identificación interno de la denuncia, junto con el acuse de recibo, para poder hacer seguimiento de ésta. A continuación, se incluye una propuesta de texto a remitir en el acuse de recibo:

Estimado/a:

Muchas gracias por ponerte en contacto con nosotros. Valoraremos la información remitida, garantizando en todo momento la confidencialidad, y nos pondremos en contacto con usted en el menor plazo posible para informarle sobre los próximos pasos. Es por ello, que le agradecemos que esté atento/a a cualquier nueva comunicación por nuestra parte.

Le saludamos atentamente,

Equipo responsable de la gestión del sistema interno de información de (nombre de la organización).

4.2 RECEPCIÓN DE LAS DENUNCIAS

El **responsable del sistema interno de información** podrá ser una persona física u órgano colegiado, y en este último caso, deberá delegar en uno de sus miembros las facultades **como responsable de la gestión del canal de denuncias y de tramitación de expedientes** de investigación[10], porque por motivos de confidencialidad el acceso a los datos personales en esta fase quedará limitado al responsable del sistema, y al encargado de tratamiento designado en caso de que la gestión del

[5] Artículo 29 Ley 2/2023.
[6] Según lo estipulado en el artículo 9.1 del REGLAMENTO (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, tendrán tal consideración: *"los datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física".*
[7] Artículo 32.2 Ley 2/2023.
[8] Artículo 7.2 Ley 2/2023.
[9] Artículo 9.2.c) Ley 2/2023.
[10] Artículo 8.2 Ley 2/2023.

canal se hubiese designado a un tercero externo[11].En caso de que el sistema interno de información integre diferentes canales de denuncia, si la persona responsable del sistema es un órgano colegiado, éste podrá delegar la gestión de cada uno de los canales de denuncia a diferentes miembros del órgano, según su perfil, o bien todos ellos a una misma persona. Por tanto, cada organización deberá acordar internamente si desea disponer de un órgano colegiado o no como responsable del sistema interno de información; aunque en organizaciones más pequeñas y ante las limitaciones de recursos, sea más pertinente que el responsable del sistema interno de información sea una única persona física, que a su vez actuará de responsable de la gestión del canal de denuncias. En caso de optar por un órgano colegiado, se recomienda que el número de miembros que lo integren sea impar a efectos de facilitar la toma de decisiones.

El responsable del sistema, y, por tanto, la persona responsable de la gestión del canal de denuncias deberá [12]:

1. Desarrollar sus funciones de forma independiente y autónoma respecto del resto de órganos de la organización, por lo que no podrá recibir instrucciones de ningún tipo en su ejercicio.

2. Disponer de todos los medios personales y materiales necesarios para llevar a cabo sus funciones.

La designación, destitución o cese, tanto del responsable del sistema interno de información (persona física u órgano colegiado) como de la persona responsable de la gestión del canal de denuncias será responsabilidad del órgano de administración o de gobierno de la organización[13].

Además, la organización podrá externalizar la recepción de las denuncias a un tercero externo, que actuará como persona encargada del tratamiento de datos personales, la cual deberá ofrecer las garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones[14].

Si la organización es privada, la(s) persona(s) responsable(s) del sistema tendrá(n) cargo de directivo/a, que ejercerá(n) su cargo con independencia del órgano de administración o de gobierno de la misma, salvo que por la naturaleza o la dimensión de las actividades de la organización no justifiquen o permitan la existencia de este cargo de forma exclusiva, en cuyo caso será posible el desempeño de las funciones del puesto de dirección con la de responsable del sistema, tratando en todo caso de evitar posibles situaciones de conflicto de interés[15]. En este último supuesto, es decir, cuando no se pueda nombrar a un(a) directivo/a específico/a para esta función o añadir esa función a un(a) directivo/a ya existente, se deberá justificar por escrito las razones por las que se opta por un perfil distinto que, en cualquier caso, deberá tener poderes suficientes y autonomía para actuar. Para seleccionar a esa persona, su perfil deberá cumplir previamente con lo siguiente:

- Tener asignada una función jerárquica por la cual asuma la responsabilidad en la organización de una especialidad profesional al completo: legal, económico, calidad, ética, etc.

- Tener autoridad para tomar algunas decisiones sobre esa especialidad.

- Incluir en su perfil laboral funciones transversales que afecten a toda la organización y que además estén relacionadas con el control, la supervisión, la auditoría, la asesoría o el seguimiento.

En ese sentido, se podrá asignar esta responsabilidad a una persona perteneciente a los cuadros de mando intermedios, tales como gerencia, coordinación de un área o departamento, o jefatura de sección. Pero, además, habrá que asignarle expresamente esta nueva función, la cual llevará reconocida la autoridad para rendir cuentas de forma directa al órgano de gobierno en los temas referidos.

En aquellas organizaciones en las que ya existiera una persona responsable de la función de cumplimiento normativo o de políticas de integridad, cualquiera que fuese su denominación, podrá ser esta la persona designada como persona responsable del sistema[16], junto con otras personas o no en función de si es un órgano colegiado el responsable del sistema, siempre que desarrolle sus funciones de forma autónoma e independiente respecto al resto de órganos de la organización.

Tanto el nombramiento como el cese de la persona física o inte-

[11] Artículo 32 Ley 2/2023. El acceso a los datos personales contenidos en el Sistema interno de información quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente a: a) El responsable del Sistema y a quien lo gestione directamente; b) El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador. En el caso de los empleados públicos, el órgano competente para la tramitación del mismo.; c) El responsable de los servicios jurídicos de la entidad u organismo, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.; d) Los encargados del tratamiento que eventualmente se designen.; e) El delegado de protección de datos.

[12] Artículo 8.4 Ley 2/2023.

[13] Artículo 8.1 Ley 2/2023.

[14] Artículo 6.2 Ley 2/2023.

[15] Artículo 8.5 Ley 2/2023.

[16] Artículo 8.5 Ley 2/2023.

grantes del órgano colegiado deberán ser notificados a la Autoridad Independiente de Protección del Informante, A.A.I., o, en su caso, a las autoridades u órganos competentes de las comunidades autónomas, en el ámbito de sus respectivas competencias, en el plazo de los diez días hábiles siguientes, especificando, en el caso de su cese, las razones que han justificado el mismo[18].

Se recomienda que la composición, tanto del responsable del sistema de información como de la persona responsable de la gestión de cada uno de los canales de denuncias que la organización tenga habilitados, quede debidamente documentada, así como en el contrato de la(s) persona(s) que asuma(n) esta responsabilidad, se incluya una cláusula de confidencialidad sobre todos los datos personales y/o informaciones vinculadas a las denuncias. A continuación, se adjunta una propuesta de contenido:

> *La persona estará obligada a guardar secreto respecto de todos aquellos datos confidenciales, personales, organizativos e informáticos de los que pudiera tener conocimiento durante la realización de sus funciones como persona responsable del sistema interno de información, y, por tanto, de todos los datos personales vinculados a las denuncias gestionadas, obligación que subsistirá aún después de haber finalizado su vinculación. Quedará, así mismo, expresamente prohibida la comunicación o la cesión de dichos datos a personas terceras, durante y después de concluida su relación con la organización, o su uso para un fin distinto al de sus funciones.*
>
> *En caso de recabar datos de carácter personal para la debida gestión de las denuncias, se obliga expresamente a solicitar información que sea acorde con la finalidad del servicio que deba prestar y evitará pedir datos, personales o no, que no sean pertinentes; o si, se recopilan por accidente, los eliminará sin dilación indebida. En cualquier caso, si la información recabada contuviera datos personales incluidos dentro de las categorías especiales de datos, procederá a su inmediata supresión, sin que se proceda al registro y tratamiento.*

En caso de que se decida externalizar la recepción de las denuncias a un tercero externo, éste actuará como encargado del tratamiento de datos personales, debiendo suscribirse el correspondiente contrato de encargo de tratamiento entre ambas partes.

[17] Ente de derecho público con personalidad jurídica propia dotado de autonomía e independencia orgánica y funcional respecto del Ejecutivo y del sector público, así como de toda entidad cuya actividad pueda ser sometida a su supervisión. Sus funciones son la llevanza del canal externo de comunicaciones, la asunción de la condición de órgano consultivo y de asesoramiento del Gobierno en materia de protección del informante, así como la elaboración de modelos de prevención de delito en el ámbito público, asunción de la competencia sancionadora en la materia, entre otros.

[18] Artículo 8.3 Ley 2/2023.

biblioteca COMPLIANCE WORLD COMPLIANCE ASSOCIATION

En aquellos casos en donde la persona física, o bien uno o varios miembros del órgano colegiado nombrado responsable del sistema interno de información tenga(n) que tomar una decisión con relación al tratamiento/investigación de una posible denuncia y esta le **afecte de forma directa y/o se encuentre ante un conflicto de interés**, la persona en cuestión no participará en la gestión del caso. En estas situaciones, se deberá otorgar a la persona informante una alternativa de comunicación, para evitar que la denuncia llegue a la(s) persona(s) con conflicto de interés directamente. Toda la información relativa a la gestión de posibles conflictos de interés en la tramitación de denuncias deberá quedar regulada en el procedimiento de gestión de las denuncias recibidas, para saber cómo actuar cuando surgen estas situaciones y cómo deberá documentarse la situación en cuestión. En el caso de que la denuncia esté relacionada con una conducta que implicase una falta muy grave -según lo establecido en el "Código de Conducta o Ético" de la organización o en el documento interno que lo regule, o en su defecto en el Estatuto de los Trabajadores u otra normativa laboral de aplicación-, por parte de la persona responsable de la gestión del canal de denuncias, durante el tiempo que dure la investigación será suspendida de forma cautelar y temporalmente -hasta que se resuelva el caso- de sus funciones como responsable de la gestión del canal de denuncias -garantizándole en todo momento sus derechos procesales como persona afectada - y se nombrará a otra persona del órgano colegiado para asumir dichas funciones de forma temporal, o en su defecto lo asumirá el órgano de gobierno.

4.3 REGISTRO DE LA DENUNCIA

Las organizaciones deberán contar con un **libro-registro** de las denuncias recibidas y de las investigaciones internas a que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad y en ningún caso se podrán conservar los datos personales durante un periodo superior a diez años . Dicho registro podrá contener el número de referencia interno asignado a la denuncia, la fecha de recepción, naturaleza de la denuncia (según catálogo interno creado), descripción de los hechos denunciados, las decisiones internas relativas al seguimiento de la denuncia, las medidas adoptadas y la fecha de cierre, entre otros.

[19] Las medidas disciplinarias deberán estar alineadas con las recogidas en el Estatuto de los Trabajadores.

[20] Artículo 26 Ley 2/2023.

Recomendamos que este registro sea responsabilidad de la persona responsable de la gestión del canal de denuncias, si bien estará a disposición del órgano colegiado responsable del sistema interno de información, en caso de haberlo, así como del órgano de gobierno. Por tanto, no será público y únicamente a petición razonada de la autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquella, podrá accederse total o parcialmente al contenido del referido registro[21].

4.4 ANÁLISIS PRELIMINAR DE LA DENUNCIA

La persona responsable de la gestión del canal de denuncias procederá a la revisión de las denuncias recibidas. Con toda la información recabada, realizará un **análisis preliminar** de los hechos denunciados, para concluir sobre la pertinencia de la misma. Como referencia para realizar dicho análisis, se podrán tener en consideración los siguientes criterios, los cuales deberán quedar debidamente documentados en el procedimiento que regula la gestión de las denuncias recibidas:

A) Nivel 1:

– ¿El hecho informado está dentro del ámbito de aplicación? Esto es, se trata de una denuncia y es relativa a la propia organización.

Para ello, es fundamental que previamente la organización defina en la política del sistema interno de información el ámbito objetivo y subjetivo del mismo (desarrolladas con profundidad en el capítulo 3 "Ámbito objetivo y subjetivo" de la presente guía). Si bien es cierto que la Ley 2/2023 se limita a las infracciones del Derecho de la Unión Europea, infracciones penales e infracciones administrativas graves o muy graves, (considerando entre éstas, en todo caso, a las que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social), así como delimita a ciertas partes interesadas las garantías de protección[22], dado el esfuerzo que supone el despliegue de este sistema, la información tan relevante que aporta para la propia organización y la confianza que aporta a sus grupos de interés, se recomienda:

- Ampliar el ámbito objetivo, entendiendo como denuncia a toda aquella comunicación sobre una conducta contraria al "Código de Conducta o Ético" de la organización, suponga ésta un acto delictivo o no. Por tanto, estarán contempladas, entre otras, las conductas recogidas en el artículo 2.1 de la Ley 2/2023:

  - Acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea.

  - Infracciones penales e infracciones administrativas graves o muy graves, considerando entre éstas, en todo caso, a las que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.

  Sin embargo, se diferenciarán de las comunicaciones que sean catalogadas como consultas, quejas o sugerencias, las cuales se remitirán al canal correspondiente para que lo gestione la unidad responsable de su debida gestión y tramitación.

  La ampliación del ámbito objetivo, entendiendo como denuncia a toda aquella comunicación sobre una conducta contraria al "Código de Conducta o Ético" de la organización, suponga ésta un acto delictivo o no, requerirá que se recabe el consentimiento explícito del denunciante para el tratamiento de los datos de carácter personal[23]. Igualmente, de ampliarse el ámbito objetivo, deberán aplicarse las garantías de protección establecida para las personas informantes protección en la Ley 2/2023 para toda la tipología de denuncias que entren a través del sistema interno de información[24].

- Ampliar el ámbito subjetivo, de modo que los canales de denuncias habilitados por la organización estén accesibles a todos los grupos de interés de la organización, aunque se podría valorar delimitar las medidas de apoyo únicamente a aquellas personas informantes que denuncien hechos contemplados en la Ley 2/2023, si bien, lo recomendable sería que no existiese tal distinción como muestra del compromiso real por parte de la organización en fomentar una verdadera cultura de cumplimiento. Para ello, es Por

[21] Artículo 26.1 Ley 2/2023.
[22] Artículo 2 Ley 2/2023.
[23] Informe jurídico 0077/2023 AEPD.
[24] Informe jurídico 0077/2023 AEPD.

tanto, en el marco de esta guía entendemos como denuncia a aquellas comunicaciones, interpuestas por cualquier grupo de interés de la organización, donde se describen unos hechos concretos, acometidos por cualquier persona vinculada a dicha organización, que la persona informante valora que pudieran ser constitutivos de incumplimiento del "Código de Conducta o Ético" de la organización, sean estos delictivos o no.

– **¿No se trata de una denuncia sobre algo ya denunciado previamente por la misma persona y sin aportar información adicional?**

B) Nivel 2: Para aquellas denuncias para las que las dos preguntas anteriores sean afirmativas, y todavía existen dudas sobre su pertinencia, así como aquellas denuncias anónimas (siempre y cuando la organización no disponga de un canal de comunicación directo con la persona informante), se aplicarán los siguientes criterios[25]:

– **Verosimilitud**: análisis del grado de credibilidad y plausibilidad de la denuncia.

– **Relevancia**: análisis del alcance, impacto, complejidad y gravedad de los hechos incluidos en la denuncia.

– **Proporcionalidad**: análisis del grado de intensidad ofensiva para un determinado bien jurídico relatado en la denuncia.

– **Motivación**: análisis del suficiente grado de detalle, rigor, justificación y coherencia de la denuncia.

Por su parte, los cuatro elementos en que deben aplicarse todos y cada uno de estos criterios son:

– **Elemento objetivo**: identificación de todos los hechos y conductas que figuran en el contenido de la alerta o denuncia.

– **Elemento subjetivo**: identificación de los sujetos que figuran; clasificación correcta de la denuncia en relación con su condición confidencial, anónima o seudónima, análisis de la intencionalidad, así como análisis de la potencial posición de vulnerabilidad en la que se pueden encontrar los sujetos afectados.

– **Elemento temporal**: identificación de los elementos temporales que figuran en el relato, revisión del momento de entrada de la denuncia, comprobación de si la presunta infracción o delito ya se ha consumado, si tiene carácter continuado o si por el contrario es un aviso de algo que se puede cometer en un futuro cercano, o bosquejo de una línea temporal más amplia en caso de varias denuncias seudónimas o confidenciales sobre el mismo asunto acontecidas con anterioridad.

– **Elemento espacial**: identificación de los puntos geográficos en los que se enmarcan los hechos denunciados o alertados, localización del lugar del presunto hecho denunciado, en la medida de lo posible identificación del lugar donde se encuentra la persona(s) afectada(s), así como contextualización de los detalles físicos y geográficos.

Resultado de ello, se propone:

- **ADMITIR LA DENUNCIA** por considerar que los hechos descritos son hechos denunciables, que pueden suponer un acto contrario al "Código de Conducta o Ético" de la organización.

- **DESCARTAR** la denuncia, en caso de que se cumplan una o más de las siguientes casuísticas:

  – Los hechos reportados no suponen un acto contrario al "Código de Conducta o Ético" de la organización.

  – Su contenido resulta irrelevante por no estar relacionado con la organización.

  – Los hechos relatados no cumplen los criterios de nivel 2 contemplados previamente.

En cualquier caso, se deberá comunicar de forma escrita a la persona informante, sobre la decisión adoptada y el motivo en caso de haber sido descartada, recomendándose que sea en el plazo máximo de diez días hábiles desde la fecha de entrada en registro de la denuncia (plazo que la Ley 2/2023 no establece de forma clara pero que, según la interpretación seguida por las personas autoras del presente

[25] "Anonimato, seudonimato y confidencialidad: Hacia un marco integral y coherente de protección de los alertadores" (David Martínez García).

documento, tomamos como referencia el mismo que se otorga a la Autoridad Independiente para admitir o inadmitir una denuncia), salvo que la comunicación sea anónima y resulte inviable la comunicación con la persona informante. En caso de que se refiera a una denuncia ajena a la propia organización, a pesar de tratarse de un hecho relevante y grave, la organización deberá descartarla al no estar dentro de su ámbito de aplicación, pero sí se recomienda prestar ayuda y orientación a la persona informante, en la medida que resulte posible, para que su denuncia prospere en los espacios donde exista la competencia requerida.

4.5 INVESTIGACIÓN DE LA DENUNCIA

Para aquellas denuncias admitidas a trámite, el responsable del sistema interno de información procederá al **nombramiento del equipo investigador** , en base a criterios de idoneidad (conocimiento técnico y del contexto, en caso de disponer) en función del tema/asunto a investigar, en caso de contar con pluralidad de perfiles. Dicho equipo será formado sobre el procedimiento que regula la gestión de las denuncias, para así asumir la responsabilidad de llevar a cabo la investigación y, por tanto, recopilar todas las evidencias y realizar las entrevistas oportunas. Las personas designadas, de forma previa a iniciar la investigación, deberán firmar una cláusula de confidencialidad la primera vez que sean nombrados miembros del equipo investigador, por lo que el responsable del sistema interno de información deberá llevar un control de las personas nombradas como equipo investigador, por denuncia y a nivel corporativo. A continuación, se adjunta una propuesta de contenido:

La persona estará obligada a guardar secreto respecto de todos aquellos datos confidenciales, personales, organizativos e informáticos de los que pudiera tener conocimiento durante la realización de sus funciones como persona miembro del equipo investigador de la denuncia nº (detallar número interno de la denuncia), obligación que subsistirá aún después de haber finalizado su vinculación. Quedará, así mismo, expresamente prohibida la comunicación o la cesión de dichos datos a personas terceras, durante y después de concluida su relación con la organización, o su uso para un fin distinto al de sus funciones.

En caso de recabar datos de carácter personal durante la investigación, se obliga expresamente a solicitar información que sea acorde con la finalidad del servicio que deba prestar y evitará pedir datos, personales o no, que no sean pertinentes para la investigación; o si, se recopilan por accidente, los eliminará sin dilación indebida. En cualquier caso, si la información recabada contuviera datos personales incluidos dentro de las categorías especiales de datos, procederá a su inmediata supresión, sin que se proceda al registro y tratamiento.

El equipo investigador deberá realizar todas las actuaciones encaminadas a comprobar la verosimilitud de los hechos relatados en la denuncia, entre otros:

– Valorar la invitación a una persona externa especialista en la materia, en caso de falta de perfiles idóneos internamente, y a otras personas de la organización que no forman parte del órgano colegiado, para avanzar con la investigación. En cualquier caso, es fundamental que el número de miembros sea el estrictamente necesario, para así limitar el acceso a información confidencial.

En este caso, los nuevos miembros deberán firmar la cláusula de confidencialidad a la que se hacía mención previamente, siempre y cuando no la hayan firmado con anterioridad.

– Solicitar nuevas evidencias y/o información tanto a la persona informante, como a otras personas a nivel interno, siempre que este hecho no ponga en riesgo la confidencialidad de la identidad de la persona informante y de la(s) persona(s) afectada(s).

– Concertar entrevistas y tomar declaración a la persona informante, a la(s) persona(s) afectada(s) y a las personas testigos, en caso de haberlas. Sin perjuicio del derecho a formular alegaciones por escrito, al que se hace mención en el apartado siguiente, la investigación comprenderá, siempre que sea posible, de una entrevista con la(s) persona(s) afectada(s) en la que, siempre con absoluto respeto a la presunción de inocencia, se le invitará a exponer su versión de los hechos y a aportar aquellos medios de prueba que considere adecuados y pertinentes, realizándose una transcripción completa y exacta de la entrevista realizada. Se ofrecerá a la(s) persona(s) afectada(s) la oportunidad de comprobar, rectificar y aceptar mediante su firma, la transcripción de la entrevista, debiendo hacer constar también la firma del entrevistador.

A fin de garantizar el derecho de defensa de la persona afectada, la misma tendrá acceso al expediente, sin revelar información que pudiera identificar a la persona informante, pudiendo ser oída en cualquier momento, y se le advertirá de la posibilidad de comparecer con una persona que sea abogada.

– Verificar la existencia o no de los hechos denunciados.

– Revisar la documentación relativa al expediente profesional de las personas implicadas, incluso de la persona informante como persona(s) afectada(s), siempre y cuando estén identificadas. Sólo se accederá a esta información cuando la información contenida en el expediente profesional esté relacionada con el hecho denunciado.

– Valorar la contratación de un análisis forense, por una persona experta externa independiente, cuando existan indicios de tratarse de un acto ilícito.

– Realizar un análisis riguroso e imparcial de la documentación disponible, con el fin de extraer una conclusión sobre los hechos denunciados, y el impacto que supone para la organización.

– Adoptar las garantías de protección oportunas.

Adicionalmente, cabe destacar que, durante todo el proceso de investigación, la identidad de las personas informantes y afectadas estará debidamente protegida, incluso una vez ésta sea finalizada, garantizando en todo momento la confidencialidad de los datos a los que hubiera tenido acceso el equipo investigador.

4.6 COMUNICACIÓN A LA(S) PERSONA(S) AFECTADA(S)

En toda investigación es fundamental velar por los **derechos que protegen a la(s) persona(s) afectadas(s)**, entre otros, la presunción de inocencia, el derecho de defensa, incluido el derecho a ser oídas, el derecho de acceso a su expediente, así como la misma protección establecida para las personas informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos personales tratados, los cuales vienen debidamente desarrollados en el capítulo correspondiente.

Así, en el curso de la investigación, se recomienda que el equipo investigador notifique a la(s) persona(s) afectada(s) en el plazo máximo de quince días hábiles desde el inicio de la investigación o desde el momento en que se conozca su identidad, si esto ocurre en un momento posterior al inicio, a través de un **correo electrónico** en el que deberá constar la siguiente información:

– Los actos y/o conductas que se le/s imputan.

– Los hechos relatados de forma sucinta.

– Todos aquellos datos que resulten relevantes para formular su defensa.

– El derecho que tiene a presentar alegaciones por escrito, así como los derechos del tratamiento de sus datos personales.

En ningún caso se comunicará a la(s) persona(s) afectada(s) la identidad de la persona informante, ni se dará acceso a la denuncia.

Esta notificación podrá retrasarse cuando la misma conlleve un riesgo por destrucción, ocultación o manipulación de las pruebas. En caso de que así sea, el equipo investigador dejará constancia de esta situación en el informe de la denuncia. En cualquier caso, dicha notificación no podrá demorarse hasta el punto de que pueda producir indefensión para la(s) persona(s) afectada(s), y, por tanto, deberá exponerse a más tardar en la entrevista a mantener con la(s) persona(s) afectada(s).

Desde la notificación a la(s) persona(s) afectada(s), se recomienda que ésta(s) disponga(n) de un plazo máximo de veinte días hábiles (plazo no estipulado en la Ley 2/2023) para **ejercer su defensa**, desde la notificación por parte del equipo investigador, argumentando por escrito cuanto crea(n) conveniente para su defensa y aportar aquellos documentos que considere(n) de interés; pudiendo contar en todo momento con el asesoramiento de la representación legal de las personas trabajadoras, en caso de haberlo, o de un abogado u abogada. Vencido el plazo sin la presentación del escrito, el equipo investigador continuará con la instrucción hasta la emisión del correspondiente informe de investigación.

4.7 EMISIÓN DEL INFORME DE LA INVESTIGACIÓN

Una vez concluidas todas las actuaciones en el marco de la investigación, el equipo investigador deberá cerrar la misma y elaborar el **informe de investigación**, el

cual se adjuntará en el libro-registro, que contendrá al menos la siguiente información:

- Código de identificación interno de la denuncia.
- Clasificación de la denuncia: acto delictivo, contrario al "Código de Conducta o Ético", y/o que supone un riesgo para la organización.
- Descripción de los hechos denunciados, indicando fecha de recepción.
- Persona(s) afectada(s), y relación de personas testigos, en caso de haberlas.
- Grupo de interés[26] de la persona informante y de la(s) persona(s) afectada(s), en caso de conocerse.
- Motivo(s) por el/los que la denuncia ha superado el análisis preliminar, y, por tanto, ha sido aceptada a investigación.
- Descripción de las actuaciones realizadas en el marco de la investigación, con el fin de comprobar la verosimilitud de los hechos.
- Conclusiones alcanzadas en la investigación, y valoración de los hechos.
- Propuesta de acciones de mejora correctivas, para eliminar las causas que han dado lugar a los hechos denunciados y prevenir su recurrencia en el futuro.
- Propuesta de medida(s) disciplinaria(s) a adoptar, en caso de que corresponda(n).

La investigación deberá concluir en un plazo máximo de tres meses, a contar desde la recepción de la denuncia o, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, éste podrá extenderse hasta un máximo de otros tres meses adicionales, debiendo quedar justificado[27].

4.8 RESOLUCIÓN Y CIERRE DE LA INVESTIGACIÓN

Una vez concluida la investigación por parte del equipo investigador, el responsable del sistema interno de información elevará a la dirección general, al órgano de administración o de gobierno de la organización o a un comité creado a tales efectos (siempre y cuando sean personas que no formen parte del órgano colegiado ni del equipo investigador de la denuncia en cuestión), en función del resultado que ofrezca dicha investigación, el informe de la investigación de la denuncia en cuestión.

Una investigación se considerará que está cerrada cuando se hayan recabado suficientes datos e información para la valoración definitiva de la denuncia. En caso de que se concluya que se ha producido una **conducta contraria al "Código de Conducta o Ético"** de la organización, la dirección general o el órgano de administración o de gobierno de la organización, según corresponda, propondrán en un plazo máximo recomendado de quince días hábiles desde el cierre de la investigación (plazo no estipulado en la Ley 2/2023), las sanciones a aplicar -según lo establecido en el "Código de Conducta o Ético" de la organización o en el documento interno que lo regule, o en su defecto en el Estatuto de los Trabajadores u otra normativa laboral de aplicación-, atendiendo a la gravedad de los hechos cometidos, y pudiendo tomar en consideración circunstancias tales como la reincidencia, el daño o perjuicios causados a las personas y a la organización. Las medidas adoptadas deberán ser debidamente notificadas a la(s) persona(s) afectada(s), y quedar registradas en el informe de la resolución o de la denuncia, en este último caso si tienen un informe único para el seguimiento de toda la denuncia.

Cuando las medidas disciplinarias sean contra una persona trabajadora, será la persona que tenga las funciones de la gestión de recursos humanos quien las gestionará, y si son contra un miembro del órgano de administración o de gobierno de la organización, será la persona que ostente la presidencia o en su defecto, la persona que ocupe la vicepresidencia quien las tramitará. En caso de que proceda la adopción de medidas legales en relación con los hechos denunciados, será la persona que tenga las funciones de la gestión de los servicios jurídicos de la organización quien los gestionará.

Si se resuelve que se ha producido una **acusación falsa** con conocimiento de dicha falsedad o hecha con el solo objeto de perjudicar a otras personas o la imagen o reputación de la organización por parte de la persona informante, **o que la información se ha obtenido ilícitamente**, la persona informante no estará amparada por las garantías de protección y perderá su derecho a la confidencialidad y no represalias. En tal caso, la organización podrá reservarse el derecho de emprender acciones legales adicionales a las medidas disciplinarias que ésta acuerde, por considerarse una falta muy grave.

[26] Entre la posible categorización, podríamos destacar, entre otros: personal laboral, personal voluntario, miembro del órgano de gobierno, persona donante, proveedor, persona socia, etc.

[27] Artículo 9.2.d) Ley 2/2023.

4.9 COMUNICACIÓN A LA AUTORIDAD COMPETENTE

La organización se reservará el derecho de **emprender** las **acciones legales** que considere oportunas contra la persona física y/o jurídica que hubiera cometido actos constitutivos de delito, primando en todo momento las libertades, derechos y protección de la(s) víctima(s). En tal caso, la dirección general o la persona en quien delegue, tras informar al órgano de administración o de gobierno de la organización, lo pondrá en conocimiento de la autoridad competente de forma inminente, poniendo a su disposición cualquier documentación y/o colaboración que fuera requerida por parte de la organización.

La información se remitirá al Ministerio cuando los hechos pudieran ser indiciariamente constitutivos de delito. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

La **identidad de la persona informante** sólo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora. Para ello, la organización deberá informar a la persona informante antes de comunicar su identidad, salvo que pudiera comprometer la investigación o el procedimiento judicial, remitiendo un escrito donde se expliquen los motivos de la comunicación de los datos confidenciales[28] .

4.10 RENDICIÓN DE CUENTAS

Dado que el órgano de gobierno es el encargado de supervisar el sistema interno de información, se recomienda que el responsable del sistema interno de información -sea persona física u órgano colegiado- eleve al órgano de gobierno un informe anual sobre el funcionamiento y eficacia del sistema, con la siguiente información, entre otras:

- Indicadores sobre número de denuncias recibidas, número de denuncias admitidas a trámite, etc.
- Tipología de los hechos denunciados.
- Medidas adoptadas de los casos investigados, una vez concluida la investigación.
- Acciones correctivas que implementar en la gestión, para eliminar las causas que han dado lugar a los hechos denunciados y prevenir su recurrencia en el futuro.
- Actualizaciones significativas del sistema interno de información.

En el caso de que las denuncias afecten a miembros del órgano de gobierno, se omitirá cierta información, siempre y cuando así se estime oportuno.

A continuación, y para facilitar la comprensión de este capítulo, se adjunta un resumen de los plazos en él mencionados:

TABLA 1. Resumen de plazos

Trámite	Plazo	Artículo Ley 2/2023
Celebración de reunión presencial, ante solicitud de la persona informante	Plazo máximo de 7 días hábiles desde su solicitud	7.2, pero no especifica si hábiles o naturales
Emisión del acuse de recibo a la persona informante	Plazo máximo de 7 días naturales desde la recepción o registro de la denuncia, salvo que pueda poner en peligro la confidencialidad	9.2.c)
Comunicación a la persona informante del resultado del análisis preliminar	Plazo máximo de 10 días hábiles desde la fecha de entrada en registro de la denuncia	No se establece
Comunicación a la(s) persona(s) afectada(s) de la investigación en curso	Plazo máximo de 15 días hábiles desde el inicio de la investigación o desde el momento en que se conozca su identidad, si esto ocurre en un momento posterior al inicio	No se establece
Ejercer la(s) persona(s) afectada(s) su defensa	Plazo máximo de 20 días hábiles para ejercer su defensa desde la notificación por parte del equipo investigador	No se establece
Cierre de la investigación	Plazo máximo de 3 meses, a contar desde la recepción de la denuncia o, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, éste podrá extenderse hasta un máximo de otros 3 meses adicionales, debiendo quedar justificado	9.2.d)
Propuesta de sanciones a aplicar	Plazo máximo de 15 días hábiles desde el cierre de la investigación	No se establece

[28] Artículo 33.3 Ley 2/2023.

CAPÍTULO 5. "*PROS Y CONTRAS DE DIFERENTES ALTERNATIVAS DE CANALES DE DENUNCIA*".

Jorge Pelegrín Saenz
Técnico de Organización y Calidad de Confederación de Salud Mental

Antes de desarrollar un argumentario acerca de las alternativas que una entidad sin ánimo de lucro tiene a su disposición para diseñar y poner a disposición de sus grupos de interés un sistema interno de información eficiente, quiero destacar las características necesarias de cualquier tipo de comunicación. Una manera conveniente de describir un acto de comunicación es la que surge de la contestación de las siguientes preguntas:

- ¿Quién?
- ¿Dice qué?
- ¿En qué canal?
- ¿A quién?
- ¿Con qué efecto?

En otros capítulos de esta guía se ha dado respuesta a **quién lo dice**, a **lo que se dice**, a **quién se dice** y, sobre todo, al **efecto** resultante **de lo que se comunica**.

En este apartado nos vamos a centrar en las características propias del canal de denuncias, que serán diferentes en función de varios aspectos de la organización, como pueden ser los siguientes:

- Su tamaño.

- Los recursos económicos que se dispone para el desarrollo del canal.

- Los recursos humanos de que se dispone para la gestión del canal.

- El grado de desarrollo tecnológico de la organización.

En cualquiera de los casos, la recomendación general de partida es que la **simplicidad y la eficiencia garanticen la salvaguardia de la persona informante**, evitando complejizar más allá de lo estrictamente necesario.

5.1 ASPECTOS DE LA ORGANIZACIÓN

En cuanto al **tamaño**, la ley de referencia ya indica la obligatoriedad de contar con un sistema interno de información a partir de un número determinado de personas trabajadoras en una organización privada[1]. En este apartado vamos a suponer que independientemente de lo que indica la Ley 2/2023, cualquier **organización** puede voluntariamente contar con un sistema interno de información, tal como está establecido en el artículo 10.2 de dicha Ley. El tamaño de la organización va a ser determinante en los otros tres aspectos para tener en cuenta ya que, a mayor tamaño es de suponer que **mayores serán los recursos económicos y humanos** que se destinarán a la gestión del canal de denuncias, y daremos por descontado que habrá un **mayor nivel de desarrollo a nivel tecnológico** para emplear lo digital en la gestión del sistema interno de información.

5.2 EMPECEMOS POR EL PRINCIPIO

Ya hemos indicado que una de las partes más importantes en un acto de comunicación es la persona que lo inicia, por tanto, debemos poner a su disposición una herramienta sencilla y accesible, que al mismo tiempo garantice que tanto su información como su persona van a ser tratados con total confidencialidad para evitar posibles represalias. Vamos a dejar aquí una serie de propuestas que pueden ser utilizadas por cualquier tipo de organización, analizando su idoneidad para cumplir con los requisitos de sencillez, accesibilidad y confidencialidad:

- **Dirección de correo electrónico:** Independientemente del tamaño y los recursos económicos o técnicos, cualquier organización puede poner a disposición de cualquier persona una dirección de correo electrónico en el que se pueda comunicar una posible denuncia. Ahora bien, en este caso, además de la dirección de correo electrónico, la persona informante debe contar con un texto en el que se le expliquen cómo se va a gestionar su denuncia, indicando quién recibe el correo, cuáles son los pasos que se van a seguir, y los plazos de respuesta a la persona que informa. Para garantizar la confidencialidad de los hechos que se describen en el correo, así como la anonimidad de la persona que los describe, se debe crear una cuenta de correo destinada en exclusiva a la gestión del canal de denuncias, que será gestionada por la persona responsable de gestionar dicho canal. Hay que destacar aquí, que existe un

[1]El artículo 10 de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre informaciones normativas y de la lucha contra la corrupción indica que las personas físicas o jurídicas con cincuenta o más trabajadores.

riesgo en la garantía del anonimato de la persona informante, ya que no se contarán con medios para evitar que una tercera parte pueda identificar a la persona informante, a partir de la identificación de la procedencia del correo electrónico desde el que envía la denuncia.

Para terminar, esta propuesta es la de mayor sencillez en cuanto a la recepción de la denuncia y de la persona informante ya que no exige grandes inversiones tecnológicas ni de recursos, pero también es la que menos garantías puede dar a la organización en cuanto a la gestión segura de la información. Por otra parte, exige a la persona responsable del canal, conocer y seguir el procedimiento de gestión interno de gestión de las denuncias.

- **Formulario de denuncia:** Podemos indicar que esta solución goza de mayor autonomía en cuanto a su gestión, además de contar con cierta automatización en los procesos. El formulario debe ser de fácil acceso a las personas informantes, y debe contar con un enlace con toda la información necesaria para que se conozca el funcionamiento del canal, ya que los formularios usuales (Google, Office 365) no cuentan con grandes espacios donde ubicar esta información, que por otra parte no haría ágil su uso. Hay que destacar que podemos configurar los formularios para que nos llegue un correo electrónico avisando de que alguien ha completado una denuncia, pudiendo así, gestionar la respuesta y el inicio de un proceso determinado. Otra de las funcionalidades de un formulario es la posibilidad de explotar los datos obtenidos, ya que todos los registros recibidos son susceptibles de exportarse a un archivo de hoja de cálculo.

- **Teléfono:** El teléfono ha sido y sigue siendo una herramienta de comunicación de amplio uso como canal de comunicación. Si decidimos su utilización en la recepción de denuncias, debemos tener en cuenta que la información que se recoja debe ser registrada, por lo que habrá que avisar a la persona informante de la pertinente grabación de datos. Esto se hará al principio de la grabación, solicitando a la persona informante el consentimiento expreso para la grabación de la conversación. La tecnología actual permite que los registros tengan la condición de archivos, por lo que tendremos que tener en cuenta que serán archivados de forma que sólo pueda acceder a ellos el responsable del sistema interno de información, para garantizar la confidencialidad de la información registrada. El uso de esta herramienta va a requerir un mayor esfuerzo a la hora de automatizar su gestión, lo que va a llevar asociado un mayor esfuerzo en recursos técnicos y humanos.

- **Aplicaciones informáticas:** Una opción interesante si contamos con recursos para ello, es la implementación de aplicaciones que nos facilitan al máximo la gestión de la información, garantizando la trazabilidad del proceso, y, por ende, la gestión de la denuncia, lo que revierte en mayor eficiencia y también en mayores garantías a la hora de demostrar la eficacia de nuestro modelo de prevención penal. Por otro lado, estas herramientas suelen tener unas medidas de seguridad técnicas que garantizan la confidencialidad, y suelen tener un diseño enfocado al cumplimiento de la Ley 2/2023, y por tanto cubren todas aquellas obligaciones inherentes al diseño del canal de denuncias, como por ejemplo ofrecer la posibilidad del anonimato u ofrecer la posibilidad de dirigir la denuncia a otra persona, del órgano colegiado si lo hay o en su defecto al órgano de gobierno, si hay un conflicto de interés con la persona responsable de gestionar el canal de denuncias, permitiendo que nos centremos en la investigación de las mismas. Existen aplicaciones del tipo CRM (*Customer Relationship Management*) o SaaS (*Software as a Service*) y otras, que permiten la completa trazabilidad de los datos registrados, ofrecen indicadores sobre el número de denuncias recibidas, porcentaje que ha sido sujeto de investigación, porcentaje de denuncias descartadas, etc. En definitiva, nos permite monitorizar el funcionamiento del canal de forma automática, permitiendo que orientemos los esfuerzos en la investigación de la denuncia. El flujo de trabajo de este tipo de aplicaciones es el siguiente: una vez que las personas informantes inician su denuncia, su mensaje queda alojado en la base de datos de la aplicación y por la automatización de sus procesos, enviará una comunicación de entrada de denuncia a la persona responsable de la gestión del canal de denuncias, acusando recibo de la recepción, procediendo también, a infor-

mar a la persona informante de plazos y procesos que seguirán a continuación. Tras estudiar la información recibida de la persona informante, dependiendo del software elegido, podrá contar con automatizaciones que mediante el cambio de estados (procede o no procede), la aplicación gestionará la información que debe enviar tanto a personas informantes, como a la persona encargada de la gestión de la denuncia: enviará un correo a la persona informante o pondrá a su disposición en la plataforma de intercambio de información una comunicación indicando si su denuncia da lugar o no, a una investigación. En el caso de que proceda iniciar una investigación, se lo comunicará a las personas designadas que llevarán a cabo la investigación, la existencia de una denuncia que debe ser investigada. Si el software elegido no contara con todas estas automatizaciones, la persona responsable de la gestión del canal deberá seguir el procedimiento interno de gestión. Estas aplicaciones suelen tener un perfil de administración, que permite dotar a la persona o personas que llevan a cabo la gestión de la denuncia, de permisos en función de la información a la que puedan acceder: contenido de la denuncia, estadísticas del canal, etc.

Entre las principales **ventajas** que ofrecen este tipo de soluciones están:

a) Permiten custodiar documentación derivada del proceso: informe de investigación, evidencias, resumen de las entrevistas, el libro-registro de actividad, que se alimenta de forma automática y que muestra todos los cambios realizados además de su autoría.

b) Permiten la comunicación bidireccional con la persona informante para solicitar más información e informarle de los avances del proceso.

c) Permiten compartir la información, con los accesos limitados según corresponda, a las personas que participen en las diferentes fases del proceso. En este caso hay que indicar que los CRM ofrecen más posibilidades de asignación de roles y permisos en detrimento de las aplicaciones de tipo SaaS, ya que cuentan con módulos de administración que permiten esta gestión de personas usuarias.

d) Permiten la traducción simultánea a diferentes idiomas.

e) Ofrecen información estadística acerca del uso del Canal de Denuncias.

f) Permiten estructurar alertas referidas a plazos de respuesta a las personas informantes; plazos para responder en cuanto a la gestión de las personas encargadas de la gestión del canal.

g) Ofrecen la posibilidad de anonimizar la información para mantener la confidencialidad de las personas informantes, o de las personas objeto de las informaciones.

La principal **desventaja** de este tipo de soluciones informáticas es la inversión económica que supone, siendo más recomendable para organizaciones que cuenten con un presupuesto destinado a infraestructura o a inversiones tecnológicas que busquen la optimización y automatización de procesos.

5.3 VALORACIÓN DE HERRAMIENTAS

A continuación, se incluye un cuadro de valoración de cada una de las soluciones aportadas en los apartados anteriores, puntuando con más o menos estrellas en función del nivel de cumplimiento de los siguientes aspectos:

- **Confidencialidad**: capacidad de la aplicación para garantizar el anonimato de la persona informante.

- **Protección de datos**: la solución empleada debe cumplir con la ley de protección de datos[2]. La persona informante debe conocer sus derechos de acceso, rectificación y cancelación, así como conocer y aceptar el tratamiento que se va a hacer de la información que aporte.

- **Comunicación entre las partes**: la solución que se utilice debe garantizar que la persona informante conozca si su información se está tramitando y, los pasos que se tomen en su gestión.

- **Registro del dato**: se debe garantizar la trazabilidad de la información, por lo que se valorará más aquella que permita mayor facilidad de acceso a la información en todos sus pasos.

[2] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Art. 6 de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre informaciones normativas y de la lucha contra la corrupción indica que las personas físicas o jurídicas con cincuenta o más trabajadores.

	Confidencialidad	Protección de datos
Teléfono	✓ ✓ ✓	✓ ✓ ✓
eMail	✓ ✓ ✓	✓ ✓ ✓
Formulario	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓
Aplicaciones Informáticas	✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓

	Comunicación entre las partes	Registro del dato
Teléfono	✓ ✓ ✓	✓ ✓
eMail	✓ ✓ ✓	✓ ✓ ✓
Formulario	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓
Aplicaciones Informáticas	✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓

Una vez la organización haya optado por la herramienta que más encaje en sus necesidades, y la haya implementado, deberá publicar en su página de inicio de la Web, en una sección separada y fácilmente identificable, información sobre el uso del canal de denuncias y los principios que rigen su sistema interno de información[3]. Para ello, se recomienda usar lenguaje sencillo, e incluso hacer uso de vídeos en diferentes idiomas (según los grupos de interés destinatarios) y de una lista de preguntas frecuentes al respecto.

[3] Art. 25 de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre informaciones normativas y de la lucha contra la corrupción indica que las personas físicas o jurídicas con cincuenta o más trabajadores.

biblioteca COMPLIANCE WORLD COMPLIANCE ASSOCIATION

6. GLOSARIO

- **Acuse de recibo:** comunicación que se envía a la persona informante, tras haber hecho uso del canal de denuncias, donde se le comunica que la entidad ha recibido su denuncia.

- **Anonimato:** Norma UNE - ISO 37002:2021 sobre Sistemas de gestión de la denuncia de irregularidades.

- **Autoridad Independiente de Protección del Informante (A.A.I):** ente de derecho público con personalidad jurídica propia dotado de autonomía e independencia orgánica y funcional respecto del Ejecutivo y del sector público, así como de toda entidad cuya actividad pueda ser sometida a su supervisión. Sus funciones son la llevanza del canal externo de comunicaciones, la asunción de la condición de órgano consultivo y de asesoramiento del Gobierno en materia de protección del informante, así como la elaboración de modelos de prevención de delito en el ámbito público, asunción de la competencia sancionadora en la materia, entre otros. A fecha de publicación de esta guía, dicha autoridad no ha sido constituida.

- **Confidencialidad:** cualidad que implica la protección y deber de secreto de la información proporcionada por la persona informante. Aunque se conoce su identidad, se toman medidas para evitar que la información se divulgue de manera inapropiada.

- **Conflicto de interés:** Un conflicto de interés en el contexto de la gestión de informaciones en los canales de denuncias se refiere a una situación en la que la objetividad y la imparcialidad de las decisiones tomadas en relación con las denuncias pueden verse afectadas debido a intereses personales y/o profesionales. Específicamente, cuando un individuo responsable de evaluar o actuar sobre una denuncia tiene conexiones o intereses que podrían influir en su juicio, se plantea un conflicto de interés. Es crucial que los responsables de la gestión de denuncias sean conscientes de posibles conflictos y tomen medidas para mitigarlos. Algunas acciones para abordar los conflictos de interés en la gestión de informaciones incluyen:

- Transparencia: Deben divulgar cualquier relación personal o profesional que puedan tener con las partes involucradas en la denuncia.

- Separación de funciones: Evitar que la misma persona que tiene un conflicto de interés tome decisiones finales sobre la denuncia.

- Procedimientos claros: Establecer procesos claros y objetivos para evaluar las denuncias, independientemente de los intereses personales.

▪ **CRM (Customer Relationship Management):** Es una tecnología que analiza y gestiona las interacciones y datos de organizaciones y personas. Orientado a un Canal de Denuncias permite centralizar y optimizar la gestión de denuncias, lo que contribuye a una cultura de transparencia y responsabilidad dentro de las organizaciones.

▪ **Denuncia:** aquellas comunicaciones, interpuestas por cualquier grupo de interés de la organización, donde se describen unos hechos concretos, acometidos por cualquier persona vinculada a dicha organización, que la persona informante valora que pudieran ser constitutivos de incumplimiento de la legislación vigente, del Código de Conducta o Ético de la organización o su normativa interna, sean estos delictivos o no.

▪ **Equipo encargado de la resolución:** es el responsable de gestionar y resolver las denuncias presentadas a través del Canal de Denuncias. Su objetivo es que se sigan los principios y valores éticos, así como proteger la privacidad de las personas involucradas en el proceso. Además, el equipo puede tomar decisiones sobre la admisión o inadmisión de las denuncias y archivarlas según corresponda.

▪ **Equipo investigador:** es un grupo de personas designadas por la persona responsable de la gestión del Canal de Denuncias que, con las debidas garantías de confidencialidad, se encargará de la investigación, de la recolección de evidencias de la denuncia y, en su caso, de la propuesta de sanción.

▪ **Informe de la investigación:** documento que elabora el órgano investigador de las denuncias, una vez que ha finalizado el proceso de investigación y en donde debe recogerse toda la información necesaria para que el equipo encargado de la resolución pueda tomar una decisión.

biblioteca COMPLIANCE WORLD COMPLIANCE ASSOCIATION

▪ **Libro- registro:** documento que deberá tener la organización para recoger y dar constancia de las denuncias recibidas e investigaciones internas realizadas.

▪ **OCDE:** La Organización para la Cooperación y el Desarrollo Económicos es una organización internacional que tiene por misión diseñar mejores políticas para una vida mejor con el objetivo de favorecer la prosperidad, la igualdad, las oportunidades y el bienestar para todas las personas.

▪ **Órgano colegiado:** consiste en un grupo formado por 2 ó más personas físicas a las que se les puede atribuir o confiar funciones de decisión, asesoramiento, seguimiento o control.

▪ **Órgano de Gobierno/ Órgano de Administración:** está integrado por un conjunto de personas encargadas de representar a la organización, del cumplimiento de los fines y de la toma de decisiones.

▪ **Persona afectada:** es la persona sobre la que se nos ha informado de la comisión de una conducta contraria a la legalidad vigente, el Código de Conducta o Ético de la organización y su normativa interna, sea ésta delictiva o no.

▪ **Persona encargada del tratamiento de datos:** es la persona sobre la que se nos ha informado de la comisión de una conducta contraria a la legalidad vigente, el Código de Conducta o Ético de la organización y su normativa interna, sea ésta delictiva o no.

▪ **Persona informante:** es la persona que nos pone en conocimiento de una denuncia.

▪ **Persona responsable del sistema interno de información:** persona física u órgano colegiado designado por el órgano de gobierno de la organización, como máximo responsable de la implementación del sistema interno de información, de garantizar que éste se implementa debidamente, velando por su cumplimiento.

▪ **Persona responsable del tratamiento de datos:** puede ser una persona física o jurídica cuya función será la de velar por el debido tratamiento de los datos personales, garantizando su protección.

▪ **Proceso de gestión de las denuncias:** es el conjunto de actividades encaminadas a asegurar la efectiva gestión de las denuncias recibidas a través de los canales de denuncias habilitados por una organización, desde su comunicación hasta su resolución final.

▪ **Represalia:** cualquier acto u omisión que esté prohibido por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, sólo por su condición de informantes.

▪ **SaaS (Software as a Service):** Es un modelo en el que las aplicaciones se ofrecen a través de Internet, directamente desde la nube. En la gestión de un Canal de Denuncias un SaaS simplifica la gestión de las denuncias al proporcionar una plataforma segura, escalable y fácil de usar. Permite la automatización de procesos en los envíos de notificaciones, así como el seguimiento del estado de las denuncias.

▪ **Sistema interno de información:** el sistema que está compuesto por todos los canales con los que cuente la organización para interponer denuncias, en caso de disponer de varios según la temática (por ejemplo, aquellas organizaciones que disponen de canales de denuncia para informar sobre posibles casos de abuso laboral y/o sexual), por la política que desarrolle los principios generales que rigen dicho sistema, y por el procedimiento que regule cómo se llevará a cabo la gestión de las denuncias recibidas, desde su recepción hasta su posible comunicación a la autoridad competente..

▪ **Softlaw:** Este concepto se refiere a principios y declaraciones que no son legalmente vinculantes. En derecho internacional, establece pautas, declaraciones de políticas o códigos de conducta, pero no son directamente exigibles.

▪ **Token CSRF (Cross-site Request Forgery):** Es un valor secreto único e impredecible generado por una aplicación del lado del servidor y enviado al cliente para su inclusión en las solicitudes HTTP posteriores emitidas por el cliente. Está diseñado para evitar ataques CSRF (falsificaciones de solicitudes entre sitios), que son vulnerabilidades comunes en aplicaciones web.

biblioteca COMPLIANCE WORLD COMPLIANCE ASSOCIATION

▪ **Token CSRF (Cross-site Request Forgery):** Es un valor secreto único e impredecible generado por una aplicación del lado del servidor y enviado al cliente para su inclusión en las solicitudes HTTP posteriores emitidas por el cliente. Está diseñado para evitar ataques CSRF (falsificaciones de solicitudes entre sitios), que son vulnerabilidades comunes en aplicaciones web.

▪ **Queja:** cualquier disconformidad, insatisfacción u observación negativa sobre la gestión y/o actuación de una organización que no está relacionada con ningún requisito de su "Código de Conducta o Ético".

▪ **Sugerencia:** cualquier aportación o comentario aportado para mejorar la gestión y/o actuación de una organización, relacionado o no con su "Código de Conducta o Ético".

▪ **Consulta:** cualquier requerimiento de información y que no conlleva acusación alguna.

biblioteca COMPLIANCE
WORLD COMPLIANCE ASSOCIATION

eqs

COMPLIANCE COCKPIT

La plataforma para programas de compliance eficaces

- Third Parties
- Whistleblowing
- Approvals
- Policies

Únase a las más de 8.000 empresas que ya generan confianza y transparencia cada día con la plataforma SaaS más segura de Europa.

World Compliance Association
Paseo de la Castellana, 79, 7º planta · 28046 Madrid · España
Tel.: 91 791 66 16 · www.worldcomplianceassociation.com

Diseño y maquetación: Equipo de diseño **WCA**

WORLD
COMPLIANCE
ASSOCIATION

biblioteca COMPLIANCE