CANALES DE DENUNCIA Y PROTECCIÓN DEL INFORMANTE EN ENTORNOS EDUCATIVOS

26 de abril de 2023

cecem madrid amepe

Índice.

1. LEY DE PROTECCIÓN DEL INFORMANTE

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 fue publicada en el BOE del 21 de febrero de 2023. Con ella se traspone la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019, conocida como Directiva *Whistleblowing*.

a. Vigencia:

Esta Ley, con **vigencia a partir del 13 de marzo de 2023**, establece la obligación de las **empresas con 50 ó más trabajadores,** y de todas las entidades públicas, de **disponer un sistema interno de información** mediante el que los trabajadores, (u otras personas que se detallan), puedan informar sobre vulneraciones del ordenamiento jurídico, y que presumirá que es "represalia" cualquier medida que se adopte respecto a un informante, que podrá tener o no una relación laboral con la empresa.

Las empresas obligadas deben implementar el sistema en **el plazo máximo de 3 meses** a partir de la entrada en vigor de la Ley; esto es, hasta el 13 de junio del presente año. **Como excepción, las entidades jurídicas privadas con plantilla entre 50 y 249 trabajadores dispondrán de plazo hasta el 1 de diciembre de 2023.**

b. Objetivo de la ley:

La regulación tiene por objeto facilitar en el seno de las empresas la comunicación de infracciones mediante la publicidad y facilitando el uso de los sistemas de información; así como asegurar la protección a los informantes. La Ley protege las informaciones y comunicaciones sobre infracciones de derecho comunitario, y sobre infracciones penales y administrativas graves o muy graves. Deben existir motivos razonables de veracidad de la posible infracción y debe encontrarse dentro del ámbito de protección de la Ley.

c. ¿A quién protege la ley?

La Ley protege a los informantes, en particular: personas trabajadoras; personas autónomas; accionistas, partícipes, miembros del órgano de administración, dirección o supervisión de una empresa; plantilla de contratistas, subcontratistas y proveedores; con relación finalizada o por comenzar, e incluso voluntarios, becarios y trabajadores en periodos de formación con o sin retribución.

Además de a los informantes, la protección de la Ley se extiende a:

- Las personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso.
- Las personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante.

- Las personas jurídicas para las que el informante trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa.

d. Sistema interno de información:

El Sistema Interno de Información, es la denominación que la Ley 2/2023 da al ya conocido como "Canal de denuncias", y lo define como el cauce preferente para informar sobre las acciones u omisiones constitutivas de infracción según la citada Ley.

Los sujetos obligados a tener un Sistema Interno de Información en el sector privado, tal como establece el artículo 10 de la Ley 2/2023 son:

- Las personas físicas o jurídicas que tengan contratados cincuenta o más trabajadores.
- Los partidos políticos, los sindicatos, las organizaciones empresariales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos.

Aunque cualquier persona jurídica podrá establecer su propio Sistema interno de información, que deberá cumplir, en todo caso, los requisitos previstos en la Ley 2/2023 y que exponemos a continuación.

e. Requisitos del Sistema Interno de información:

Con carácter general, el Sistema Interno de Información deberá cumplir con los siguientes requisitos:

- Plazos del procedimiento: En el plazo de 7 días desde la recepción de la información o comunicación se deberá acusar recibo al informante. La gestión e investigación de las informaciones o comunicaciones no podrá durar más de 3 meses, salvo casos de especial complejidad, en cuyo caso podrá prorrogarse 3 meses más.
- Información y publicidad: Las empresas estarán obligadas a dar información y publicidad sobre el uso del canal interno y sobre los principios esenciales de su procedimiento de gestión. En caso de tener la empresa página web, el canal deberá aparecer en la página de inicio, en sección separada fácilmente identificable.
- Responsable: Será un directivo de la empresa nombrado por el órgano de administración, debiendo ejercer su cargo con independencia. Podrá asumir la función de responsable del sistema el “compliance officer” o responsable de cumplimiento normativo si lo hubiera.

Y en relación al canal interno de información, es decir, el medio por el que se reciba la información, los requisitos son:

- Ha de permitir realizar comunicaciones por escrito (correo postal o a través de cualquier medio electrónico) o verbalmente (por vía telefónica o a través de sistema de mensajería de voz), o de las dos formas. A solicitud del informante, también

mediante reunión presencial dentro del plazo máximo de siete días (informando de que la comunicación será grabada y del tratamiento de sus datos conforme al RGPD).

- Ha de posibilitar la presentación y posterior tramitación de comunicaciones anónimas.
- No obtendrá datos que permitan la identificación del informante y deberán contar con medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado.
- Se ha de informar a los usuarios del canal de la posibilidad de indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones y sobre los canales externos de información ante las autoridades competentes.

f. Responsable de la implantación del Sistema Interno de Información

El órgano de administración u órgano de gobierno de cada entidad u organismo obligado por la ley 2/2023 será el competente para la designación de la persona física, u órgano colegiado, responsable de la gestión de dicho sistema o «Responsable del Sistema», y de su destitución o cese.

Tanto el nombramiento como el cese de la persona física individualmente u órgano colegiado designado deberán ser notificados a la Autoridad Independiente de Protección del Informante, A.A.I.

El Responsable del Sistema persona física u órgano colegiado serán directivos de la entidad, y ejercerán su cargo con independencia del órgano de administración o de gobierno de la misma. Cuando la naturaleza o la dimensión de las actividades de la entidad no justifique o permita la existencia de un directivo Responsable del Sistema, será posible el desempeño ordinario de las funciones del puesto o cargo con las de Responsable del Sistema, tratando en todo caso de evitar posibles situaciones de conflicto de interés.

El Responsable del Sistema deberá desarrollar sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad, no podrá recibir instrucciones de ningún tipo en su ejercicio, y deberá disponer de todos los medios personales y materiales necesarios para llevarlas a cabo.

En las entidades u organismos en que ya existiera una persona responsable de la función de cumplimiento normativo o de políticas de integridad, cualquiera que fuese su denominación, podrá ser esta la persona designada como Responsable del Sistema, siempre que cumpla los requisitos establecidos en la ley 2/2023.

g. Gestión del Sistema Interno de Información

El órgano de administración u órgano de gobierno de cada entidad u organismo obligado por la ley 2/2023 aprobará el **procedimiento de gestión de informaciones**. El Responsable del Sistema responderá de su tramitación diligente.

En particular, el procedimiento de gestión responderá al contenido mínimo y principios siguientes:

- Identificación del canal o canales internos de información a los que se asocian.
- Inclusión de información 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.
- Envío de acuse de recibo de la comunicación al informante, en el plazo de siete días naturales siguientes a su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.
- Determinación del plazo máximo para dar respuesta a las actuaciones de investigación, que no podrá ser superior a tres meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante, a tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación, 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.
- Previsión de la posibilidad de mantener la comunicación con el informante y, si se considera necesario, de solicitar a la persona informante información adicional.
- Establecimiento del derecho de la persona afectada a que se le informe de las acciones u omisiones que se le atribuyen, y a ser oída en cualquier momento. Dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.
- Garantía de la confidencialidad cuando la comunicación sea remitida por canales de denuncia que no sean los establecidos o a miembros del personal no responsable de su tratamiento, al que se habrá formado en esta materia y advertido de la tipificación como infracción muy grave de su quebranto y, asimismo, el establecimiento de la obligación del receptor de la comunicación de remitirla inmediatamente al Responsable del Sistema.
- Exigencia del respeto a la presunción de inocencia y al honor de las personas afectadas.
- Respeto de las disposiciones sobre protección de datos personales.
- Remisión de la información al Ministerio Fiscal con carácter inmediato 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 **gestión de la información** se podrá llevar a cabo:

- Dentro de la propia entidad u organismo o
- Acudiendo a un tercero externo, que tendrá la consideración de encargado del tratamiento a efectos de la legislación sobre protección de datos personales y que, a

la hora de su elección, habrá de ofrecer al responsable las garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones. Dicho tratamiento se regirá por el acto o contrato del artículo 28.3 del RGPD.A estos efectos, se considera gestión del Sistema la recepción de informaciones.

h. El Registro de Informaciones

Los sujetos obligados a disponer del canal de información deben contar con un libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad previstos en la Ley.

- No se trata de un registro público. Únicamente a petición razonada de la Autoridad judicial competente, mediante auto, en el marco de un procedimiento judicial, podrá accederse total o parcialmente al contenido del mismo.
- Los datos personales relativos a las informaciones recibidas y a las investigaciones internas se conservarán únicamente:
    - durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.
    - Si la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se conservará mientras se tramite el procedimiento judicial.
    - En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema.
    - Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo del art. 32 de la LOPDGDD.
    - En ningún caso podrán conservarse los datos por un período superior a diez años.
- Los empleados y terceros deberán ser informados acerca del tratamiento de datos personales en el marco de los Sistemas de información.

i. Plazo máximo para el establecimiento de Sistemas internos de información y adaptación de los ya existentes

- Las **personas físicas o jurídicas del sector privado** que tengan contratados entre cincuenta y doscientos cuarenta y nueve trabajadores tienen de plazo **hasta el 1 de diciembre de 2023.**

- **El resto de entidades obligadas**, como las empresas con doscientos cincuenta (250) o más trabajadores y las organizaciones empresariales y las fundaciones creadas por ellas que reciban o gestionen fondos públicos, **hasta el 13 de junio de 2023.**

j. La Autoridad Independiente de Protección del Informante, A.A.I.

Para garantizar una adecuada protección del informante (en cumplimiento de la Directiva 2019/1937) se ha de disponer de un completo marco normativo-institucional con el que dar respuesta a dicha necesidad de protección.

En ese marco, el legislador ha considerado conveniente:

- La creación de una nueva entidad que garantice la funcionalidad del sistema, la Autoridad Independiente de Protección del Informante, A.A.I., como 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 (similar, en este aspecto, a la AEPD)
- La articulación de un canal externo de información que complementa los canales internos (tanto en el sector privado como público)

Será la AAI la encargada de la llevanza y gestión del citado canal externo.

k. Protección de datos:

El tratamiento de datos personales que derive de la aplicación de esta ley están sujetos a la normativa sobre protección de datos (RGPD, LOPDGDD y LO 7/2021)

<u>La licitud del tratamiento resulta:</u>

- del cumplimiento de una obligación legal (para los sistemas internos de información obligatorios y canales de comunicación externos)
- del interés público (para los sistemas internos de información voluntarios y supuestos de revelación pública)
- del interés público esencial (para el tratamiento de categorías especiales de datos)

Es obligatorio cumplir el deber de información de los datos del responsable de tratamiento de datos en los términos establecidos en los artículos 13 RGPD y 11 de la LOPDGDD, cuando los datos personales se obtengan directamente de los interesados.

A los informantes y a quienes lleven a cabo una revelación pública se les informará, además, de forma expresa, de que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.

La identidad del 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.

La persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante o de quien haya llevado a cabo la revelación pública.

Los datos personales que no sean necesarios para el conocimiento e investigación de hechos o que se refieran a conductas no incluidas en el ámbito de aplicación de la ley habrán de ser inmediatamente suprimidos.

Los derechos de los interesados son los recogidos en artículo 15 del RGPD:

- En relación con la persona a la que se refieran los hechos relatados: se presumirá, salvo prueba en contrario, que existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales, por lo que no podrán ejercer el derecho de oposición.

Únicamente podrán tener acceso a los datos personales contenidos en el Sistema interno de información:

- El Responsable del Sistema y quien lo gestione directamente.
- El responsable de RRHH, solo cuando proceda la adopción de medidas disciplinarias contra un trabajador.
- El responsable de los servicios jurídicos de la entidad, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.
- Los encargados del tratamiento que eventualmente se designen (por ejemplo, servicios jurídicos externos contratados para evaluar jurídicamente la información facilitada a través del canal).
- El Delegado de Protección de Datos.

No obstante, será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

l. Protección al informante:

Durante dos años, el informante estará protegido frente a las medidas que pudieran adoptarse como represalia por la información revelada.

Cuando el informante haya demostrado razonablemente que ha comunicado o ha hecho una revelación pública y que ha sufrido un perjuicio, se presumirá en los procedimientos judiciales que el perjuicio se produjo como represalia, y corresponderá a la persona que haya tomado la medida perjudicial probar que esa medida se basó en motivos justificados ajenos a la comunicación o revelación pública.

Los actos constitutivos de represalia serán nulos y darán lugar a medidas disciplinarias o de responsabilidad, incluyendo una indemnización de daños y perjuicios.

m. Régimen sancionador:

Tendrán, entre otras, la consideración de infracciones muy graves:

- La **limitación, a través de contratos o acuerdos, de los derechos y garantías previstos en la ley**; cualquier intento o acción efectiva de obstaculizar la presentación

de comunicaciones; o de impedir, frustrar o ralentizar su seguimiento, incluida la aportación de información o documentación falsa.
- La adopción de **represalias** frente a informantes y demás sujetos protegidos.
- **Vulnerar** las garantías de **confidencialidad y anonimato**, en particular del informante que haya optado por la misma.
- **Vulnerar el deber de secreto** de cualquier otro aspecto relacionado con la información.
- **Comunicar o revelar públicamente información a sabiendas de su falsedad**.
- **Incumplimiento de la obligación de disponer de un Sistema interno de información** en los términos exigidos en esta ley.

La comisión de infracciones anteriores llevará aparejada la imposición de las siguientes multas:

- Si son personas físicas las responsables de las infracciones: **de 30.001 hasta 300.000 euros**.
- Si son personas jurídicas: **entre 600.001 y 1.000.000 de euros**. Estas **podrán ser publicadas en el «Boletín Oficial del Estado»**, tras la firmeza de la resolución en vía administrativa

Adicionalmente, la **A.A.I.** podrá acordar:

- La **amonestación pública**.
- La **prohibición de obtener subvenciones u otros beneficios fiscales** durante un plazo máximo de cuatro años.
- La **prohibición de contratar con el sector público** durante un plazo máximo de tres años.

2. CANAL DE DENUNCIAS

a. Normativa aplicable

Los países miembros de la UE deben adaptarse a la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019 y poner en marcha una normativa que garantice la prevención de delitos internos en la empresa, así como la protección a los denunciantes.

De acuerdo a 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, las empresas con 50 o más empleados deben cumplir con la obligación del canal de denuncias e implementar esta herramienta, siguiendo los requisitos dispuestos por la normativa.

Además de ésta, hay otras leyes que obligan a las empresas a tener implementado un canal de denuncias, como son el Código Penal, que establece el canal de denuncias como requisito del plan de prevención de delitos penales, la Ley de Igualdad dentro de los planes de

igualdad, la Ley de Blanqueo de Capitales o la Ley de protección integral de la infancia y la adolescencia para empresas del ámbito deportivo, ocio o educativo que cuenten con la presencia de menores.

Así mismo, cualquier empresa que decida adoptar la norma ISO 37301 sobre sistemas de gestión de compliance, también tiene la obligación de implementar un canal de denuncia interno.

Del mismo modo, las empresas obligadas a implementar un canal de denuncias también deben designar un Delegado de Protección de Datos obligatorio, ya que deben tenerlo todas las empresas con más de 50 trabajadores que traten datos sensibles o que puedan poner en riesgo la privacidad, seguridad o integridad de los interesados.

b. ¿Qué es el canal de denuncias?

El canal de denuncias para empresas es la vía de comunicación interna a través de la cual la empresa recibe y gestiona las denuncias (o comunicaciones) hechas por los miembros de la propia empresa o por otras personas vinculadas a ella, sobre posibles conductas irregulares o ilícitas de las que puedan haber sido testigos o tengan conocimiento y que sean contrarias a las normas de la empresa, tanto internas como externas.

Por lo tanto, el canal de denuncias en las empresas es una herramienta que permite detectar comportamientos irregulares o ilícitos dentro de la propia empresa, ya sean estos contra normativas nacionales o internacionales vigentes o contra la propia normativa interna de la empresa. A través del canal de denuncias interno, los miembros de la empresa y aquellas personas externas, pero vinculadas a la misma, pueden denunciar dichos comportamientos, para que el correspondiente órgano o comité trámite y, en su caso, investigue las denuncias recibidas.

El canal de denuncias interno es una herramienta esencial de cualquier plan o programa de compliance o cumplimiento normativo y un requisito del plan de prevención de delitos penales, tal y como recoge 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 el artículo 31 bis del Código Penal. Por ello, la relación entre canal de denuncias y compliance es evidente, sin el primero tendríamos un sistema de gestión de compliance insuficiente y, seguramente, ineficiente.

A la hora de gestionar el canal de denuncias de la empresa resulta imprescindible contar con la figura del Delegado de Protección de Datos, ya que se trata de información altamente confidencial y que puede suponer riesgos para los interesados, tanto para el denunciante como para el trabajador objeto de la denuncia.

c. ¿Cuáles son las ventajas del Canal de denuncias en la empresa?

La implementación de un canal de denuncias en las empresas, más allá del cumplimiento de la ley, aporta una serie de ventajas a las organizaciones, entre las que destacamos:

- Una detección temprana de conductas delictivas o ilícitas, pudiendo ponerles freno antes de que sean más graves y supongan mayores daños para la empresa, tanto económicos como reputacionales.
- Si la infracción o el delito se produce, contribuye a reducir el impacto negativo en la reputación e imagen de la empresa y puede atenuar o eximir la responsabilidad penal de la misma (siempre que se pruebe que el canal de denuncias es efectivo).
- Al poder presentar denuncias anónimas, aumenta las posibilidades de que más miembros de la empresa recurran a este medio para denunciar conductas ilícitas u otros comportamientos nocivos, como el acoso.
- La investigación y sanción interna permite resolver problemas dentro de la empresa, sin llegar a los tribunales (siempre y cuando no se trate de delitos penales, en cuyo caso deben ser denunciados) y, por tanto, incluso sin que llegue a trascender públicamente, lo que minimiza el impacto en la reputación de la empresa.
- Favorece y promueve una cultura ética y transparente dentro de la empresa.

d. ¿Para qué sirve el canal de denuncias interno en la empresa?

Podemos decir que el canal de denuncias en empresas sirve para cumplir con dos finalidades; por un lado, persigue la comisión de delitos e infracciones en el desarrollo de las actividades de las empresas y, por otro lado, proteger de una manera mucho más efectiva a los informantes.

Desde su finalidad como sistema para prevenir y perseguir la comisión de delitos e infracciones, el canal de denuncias interno busca cumplir con los siguientes objetivos:

- Detectar de forma anticipada posibles irregularidades o conductas contrarias a la ley o la normativa interna de la empresa.
- Combatir la comisión de irregularidades o delitos en las siguientes áreas:
    - Contratación pública
        - Competencia
        - Servicios financieros
        - Protección del medio ambiente
        - Seguridad nuclear
        - Sanidad animal
        - Seguridad de los productos, de los alimentos y del transporte
        - Salud pública
        - Protección de los consumidores
        - Protección de datos y privacidad
        - Mercado interior e intereses financieros de la UE
        - Fraudes y estafas
        - Blanqueo de capitales
        - Irregularidades con la Seguridad Social o la Agencia Tributaria

- Demostrar la eficacia del sistema de gestión de compliance y los controles del mismo.
- Hacer un uso apropiado del régimen disciplinario de la empresa y castigar a quienes cometen irregularidades o conductas ilícitas dentro de la misma.
- Colaborar con la investigación judicial, si se produce un procedimiento penal relativo a la empresa.
- Atenuar o eximir la responsabilidad penal de la empresa, en el caso de que se haya cometido un delito por parte de uno de sus miembros.

Como decíamos, la otra finalidad del canal de denuncias es proteger a los informadores de cualquier forma de represalia en su contra, con el fin de que más personas se decidan a dar el paso y denunciar aquellas irregularidades o comportamientos en contra de la ética y la normativa interna de la organización.

e. ¿Cómo debe ser el modelo del canal de denuncias?

Cualquier modelo de canal de denuncias debe cumplir con una serie de requisitos para que resulte eficiente, pero sobre todo confiable, ya que los denunciantes deben ser protegidos de cualquier posible represalia y su identidad preservada (tanto si la denuncia es anónima como si no lo es). Esto se consigue si:

- El procedimiento del canal de denuncias es transparente, es decir, se ha definido con claridad qué se puede denunciar, cómo se debe presentar y formalizar la denuncia, cómo se tramitará la denuncia y qué órgano está encargado de cada parte del proceso, que se debe dividir en: recepción, investigación, valoración de la sanción y ejecución de la sanción. Si es posible y el tamaño de la empresa lo permite, cada una de esas partes las llevará a cabo un órgano de diferente, garantizando así una mayor imparcialidad durante todo el proceso.
- El canal de denuncias es fácil de usar, es decir, es fácil acceder a él desde diferentes dispositivos y presentar una denuncia a través de la vía o vías habilitadas para ello.
- Se ha comunicado la existencia del canal de denuncias a los trabajadores y explicado cómo debe usarse, cómo se protegerá a los denunciantes y se asegurará la confidencialidad durante todo el proceso.
- Se asegura la protección del denunciante y del denunciado. Del primero ante posibles represalias y del segundo ante posibles denuncias falsas o malentendidos que hayan derivado en una denuncia.
- Cuenta con indicadores que permitan valorar y evaluar su funcionamiento y eficacia.

- Se garantiza la protección de datos, aplicando las medidas de seguridad técnicas y organizativas necesarias para garantizar la confidencialidad de denunciantes y denunciados.

Modelo de canal de denuncias	
Definición de la política del canal (debería ser negociada previa consulta o negociación con la representación legal de las personas trabajadoras)	-Ámbito de aplicación (la empresa o empresas que conformen el grupo. -Qué conductas y acciones se pueden denunciar -Quién puede denunciar (empleados, proveedores, socios, etc.) -Contenido mínimo de las denuncias -Vías para presentar las denuncias -Procesos de gestión e investigación de las denuncias -Protección de datos del canal
Definición del órgano u órganos que gestionarán el canal y las denuncias (definir si la gestión será interna, externa o mixta)	-Órgano de compliance y sus funciones -Recepción de denuncias -Clasificación de denuncias (archivo o tramitación) -Apertura de expediente e investigación interna -Informe de conclusiones -Adopción de medidas disciplinarias -Notificación a las partes (denunciante y denunciado)
Implementación del canal	-Diseño -Reglamento -Procesos
Comunicación del canal	-Comunicación de la existencia y alcance del canal a toda la empresa -Formación sobre la existencia, uso y características del canal -Publicación del reglamento del canal
Seguimiento	-Supervisión y evaluación del funcionamiento del canal (uso de indicadores para su valoración)

f. ¿Cómo articular el canal de denuncias?

A continuación ofrecemos una breve información sobre los 6 mejores software para implantar un canal de denuncias

<u>iThikios</u>

Este software para canal de denuncias anónimas permite cumplir con todas las exigencias de la nueva ley europea sobre whistleblowing, y aplicar el compliance laboral, penal y legal de forma efectiva en la empresa.

Se trata de una herramienta en la nube, segura y muy sencilla de utilizar. Su configuración estará lista en apenas unos minutos, sin necesidad de recurrir a programadores o expertos en diseño de aplicaciones.
El programa está totalmente adaptado a la normativa vigente de protección de datos. Gracias a él se puede actuar con la máxima transparencia con clientes, empleados, proveedores o socios comerciales.

Egrity LineQS Inte

Este software para implantar un canal de denuncias es uno de los más utilizados a nivel mundial, no en vano ha sido el elegido por más de 1.200 empresas en 165 países.
La herramienta de EQS Integrity Line ofrece a los alertadores la posibilidad de denunciar casos de corrupción, blanqueo de capitales, abusos de autoridad, discriminaciones en la empresa y cualquier otro comportamiento ilícito o inapropiado en la organización. Y todo ello con información encriptada, de forma que se garantiza el total anonimato, tal y como marca la Directiva whistleblowing.
A través de esta herramienta se puede digitalizar por completo el canal de denuncias de la empresa, y favorecer una cultura organizacional ética y transparente. Además, está disponible en diferentes versiones según las necesidades de cada empresa (Essential, Best Practice y Enterprise).

Whistlelink

Whistlelink es un software para canal de denuncias que destaca por su gran versatilidad y sencillez de uso. Está disponible en 20 idiomas y puede ser configurado en apenas 10 minutos.
Con Whistlelink cualquier empresa puede crear un canal de denuncias seguro. La información proporcionada por los alertadores y que albergan sus servidores en Suecia está totalmente encriptada, por lo que el anonimato está siempre garantizado.
Esta herramienta cuenta con todo lo necesario para adaptarse a la nueva Directiva Whistleblowing. Y sino, siempre puedes descargarte la versión de prueba totalmente gratis.

WhistleB

WhislteB ofrece una canal de denuncias seguro, fácil de usar y orientado a los clientes. Está diseñado para cumplir con la norma UNE 27001, con la directiva europea sobre whistleblowing y con el Reglamento General de Protección de Datos (RGPD).
Permite crear diversos canales de denuncias diseñados a la medida de las exigencias y necesidades de cada empresa. En concreto cuenta con tres planes: el Core es el básico, está disponible en tres idiomas y permite crear un canal de denuncias; el Pro está disponible en 15 idiomas y permite crear dos canales de comunicación; por último, el Premium es ideal

para grandes empresas, ya que está disponible en 30 idiomas y permite hasta cinco canales de comunicación.

Centinela Canal de denuncias

Centinela es otro de los software para compliance más conocidos. Está desarrollado por Lefevbre y, entre sus muchas opciones, está la posibilidad de crear un canal de denuncias interno seguro dentro de la empresa.

Esta herramienta permite crear un sistema de alertas que avisa cuando se comete alguna irregularidad. Asimismo, guarda de manera automática todos los procesos abiertos y realiza un seguimiento en tiempo real de todas las denuncias. También permite crear y descargar informes sobre cada caso.

Otro de los grandes puntos fuertes de este software es que cuenta con un alto nivel de seguridad, de hecho está certificado según la norma ISO 27001.

El software Centinela para canal de denuncias se puede descargar desde la propia web de Lefebvre. Está disponible en tres versiones (Pro, Plus y Premium). También se puede solicitar una demo de prueba gratuita.

GlobalSUITE Solutions

El software para canal de denuncias GlobalSUITE Solutions es otro de los más recomendables a la hora de detectar y denunciar irregularidades en una empresa.

Al igual que el resto de programas de nuestra lista, esta herramienta permite que las empresas gestionen de forma rápida, sencilla y automatizada todas las denuncias e irregularidades que se puedan cometer en su seno.

De nuevo, es un programa que destaca por garantizar unos altos niveles de protección y seguridad, permitiendo a los alertadores realizar las denuncias de forma totalmente anónima y confidencial.

En definitiva, todos estos software para canal de denuncias son ideales para garantizar el cumplimiento de la Directiva 2019/1937 sobre whistleblowing en tu empresa. Antes de decidirte por uno te recomendamos ponerte en contacto con sus asesores comerciales para que te cuenten de forma detallada las características del programa, o descargar sus demos gratuitas para probarlos y comprobar cuál se adapta mejor a tus necesidades.

g. gestión externa del canal: propuesta de CECE-Nacional

Modalidad

Desde que la Ley 2/2023 fue publicada en el BOE nº 44 de 21 de febrero, la CECE-Nacional ha tenido el firme propósito de asistir a los centros en la implantación del Sistema interno de información.

Dicha asistencia, que empezó siendo meramente informativa ha evolucionado hasta ofrecer, a todos aquellos centros que hayan designado a CECE como Delegado de Protección de

Datos (DPD) para el desempeño de las funciones del art. 39 del RGPD, SIN COSTE ADICIONAL ALGUNO, la posibilidad, si así lo desean, de llevar a cabo la"gestión externa del sistema interno de información", entendiendo "gestión" en los términos que menciona el art. 6 de la Ley 2/2023, de recepción de informaciones. Dicho ofrecimiento obedece a un doble fin:

- por un lado, ofrecer garantías adecuadas al informador de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones y crear en él el adecuado clima de confianza, reforzado por la condición de DPD de la CECE.
- por otro, evitar a los centros el tener que incurrir en el gasto adicional que supondría el acudir a un nuevo tercero en caso de optar por la gestión externa del canal.

Esta oferta de gestión externa del sistema interno de información ha llevado al Dpto. de Protección de Datos de CECE (y en ese proceso está a día de hoy) a tener que elaborar los diversos textos que dicha implantación conlleva: desde la bienvenida al Canal, con la información sobre protección de datos que ha de figurar cuando se accede al canal, y sobre el uso del mismo al informante, hasta el procedimiento de gestión del Sistema, el Registro de informaciones o la información a proporcionar a trabajadores y terceros sobre el tratamiento de sus datos personales, entre otros.

La modalidad seleccionada por CECE para la recepción de las informaciones en la gestión externa del Canal es la del correo electrónico y, por lo tanto, la de la comunicación por escrito. Para ello tomará como punto de partida la página web del Centro.

El art. 25 de la Ley 2/2023 señala que "*En caso de contar con una página web, dicha información (en referencia a la información clara y fácilmente accesible sobre el uso del canal interno de información y , sobre los principios esenciales del procedimiento de gestión) deberá constar en la página de inicio, en una sección separada y fácilmente identificable*".
Por tanto, en el footer de la web del Centro, junto al Aviso Legal y la diferentes Políticas (Privacidad, Protección de Datos y Cookies) deberá figurar un apartado denominado "*Canal de Denuncias" (o Sistema de Información).*
Cuando el usuario/informante pinche en el enlace "Canal de denuncias" (como se ve en la imagen superior) éste ha de llevarle a un espacio en la web del Centro (https://colegioaxxx.es/canal-d... p.ej), en el que se le dará la bienvenida al canal, se le explicará el procedimiento de gestión del mismo y sus principios esenciales y se le facilitará

información en materia de protección de datos. Estos textos serán redactados por CECE y facilitados al Centro para que quien gestione su web los inserte en dicho espacio, siguiendo siempre las instrucciones de CECE.

Es aquí donde CECE ofrecerá a los centros dos opciones (a elegir una de ellas antes de la implantación). Que junto a la información anterior, en dicho espacio:

- Se inserte un formulario (cuyos campos determinará CECE, conforme a la Ley 2/2023) y que debería posibilitar el poder adjuntar documentos (como se hace con los CVs)
- No se inserte formulario alguno, y simplemente se facilite una dirección de email de CECE, del tipo gestionexterna.canaldenuncias@cece.es. En este caso el informante mostraría su email como remitente, cosa que no ocurriría necesariamente con el método del formulario.

De optar el Centro por insertar un formulario, cuando el informante pinche en "ENVIAR", el sistema habrá de dirigir toda la información a la dirección de email de CECE gestionexterna.canaldenuncias@cece.es El formulario deberá ser creado (siguiendo las instrucciones de CECE) y alojado por cada centro, que deberá configurar dicho formulario para que la cuenta receptora del contenido sea gestionexterna.canaldenuncias@cece.es

Gestión externa del canal por parte de CECE-Nacional

CECE se ocupará de la recepción de la información enviada a la dirección gestionexterna.canaldenuncias@cece.es y, preservando en un primer momento la identidad del informante (en el caso de que se identificara o facilitara email):

- Conforme a la Ley 2/2023, redactará y enviará acuse de recibo de la comunicación al informante (en el caso de que fuera posible) y demás información precisa.
- Contactará con el Responsable del Sistema que hubiera designado el Centro o la entidad titular del mismo) y:
    - Le informará de la recepción.
    - Aunque excede del ámbito propio de lo que es la "gestión externa" del canal, la CECE emitirá (verbalmente o por escrito) una primera valoración jurídica de las acciones u omisiones de las que se informa
    - Le remitirá, empleando los medios de seguridad que cada caso requiera, la información recibida.

Servicio de asistencia jurídica que vaya más allá de la gestión externa del Canal

En CECE queremos acompañar a los Centros durante todo el proceso que, si se estimara que las acciones u omisiones de las que se informa pudieran ser constitutivas de delito, culminaría con la remisión de la misma al Ministerio Fiscal o, en el caso de que los hechos afectaran a los intereses financieros de la Unión Europea, a la Fiscalía Europea.

En principio, dicha asistencia comprendería:

- Elaborar de un **informe jurídico preliminar** (en base a la información recibida)
- **Asistir al centro en las actuaciones de investigación**.
- **Garantizar la presunción de inocencia y el honor de las personas afectadas**, así como el derecho a que se le informe (en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación) de las acciones u omisiones que se le atribuyan, y que pueda ser oída en cualquier momento.
- **Asistir al centro en la remisión de la información al Ministerio Fiscal** cuando los hechos pudieran ser indiciariamente constitutivos de delito.

Los términos y condiciones finales en los que CECE prestaría este servicio de asistencia jurídica están siendo objeto de estudio. Esperamos poder comunicarlos a los centros **antes del 13 de junio**.

Actualizado a 26 de abril de 2023

Puedes escribirnos a comunicacion@cecemadrid.es

Consulta nuestros servicios y más materiales en

www.cecemadrid.es