POLÍTICA DEL CENIEH EN MATERIA DE SISTEMA INTERNO DE INFORMACIÓN Y DEFENSA DEL INFORMANTE

INTRODUCCIÓN.

El 21 de febrero se publicó en el B.O.E, 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 (en adelante "la Ley"). Dicha Ley incorpora al Derecho español la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, la cual regula aspectos mínimos que han de satisfacer los distintos cauces de información a través de los cuales una persona física que sea conocedora en un contexto laboral de una infracción del Derecho de la Unión Europea, pueda dar a conocer la existencia de la misma.

La finalidad de la Ley es otorgar una protección adecuada frente a las represalias que puedan sufrir las personas físicas informantes a través de los procedimientos previstos en la misma, así como fortalecer la cultura de la información, de las infraestructuras de integridad de las organizaciones y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público.

I.- EL SISTEMA INTERNO DE INFORMACIÓN DEL CENIEH.

El Consorcio CENIEH (en adelante CENIEH), adscrito a la Administración General del Estado, y como una entidad de derecho público integrada por la Administración General del Estado, a través del Ministerio de Ciencia, Innovación y Universidades, y por la Administración General de la Comunidad de Castilla y León, a través de la Consejería de Educación, está obligado a disponer de un sistema interno de información que cumpla con todos los requerimientos de la Ley, entre otros, su uso asequible, las garantías de confidencialidad, las prácticas correctas de seguimiento, investigación y protección del informante, y la designación del responsable de su correcto funcionamiento,

El sistema interno de información es el cauce preferente para informar de las acciones y omisiones previstas en la Ley, siempre que se pueda tratar de manera efectiva la infracción y si el informante considera que no hay riesgo de represalia.

El CENIEH proporcionará de forma clara y fácilmente accesible la información adecuada sobre el uso de todo canal interno de información que implante, así como sobre los principios esenciales del procedimiento de gestión. Dicha información deberá constar en la página de inicio de su página web, en una sección separada y fácilmente identificable.

II.- ÁMBITO MATERIAL DE APLICACIÓN DEL SISTEMA INTERNO DE INFORMACIÓN DEL CENIEH.

El sistema permitirá presentar, a través del canal interno, información sobre las siguientes materias:

a) Cualesquiera acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea en las materias de Contratación pública, Servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo, Seguridad de los productos y conformidad, Seguridad del transporte, Protección del medio ambiente, Protección frente a las radiaciones y seguridad nuclear, Seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales, Salud pública, Protección de los consumidores, Protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información; o afecten a los intereses financieros de la Unión Europea; o incidan en el mercado interior, incluidas las infracciones de las normas de la Unión Europea en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades o con prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades.

b) Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave. En todo caso, se entenderán comprendidas todas aquellas infracciones penales o administrativas graves o muy graves que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.

c) Cualesquiera otras informaciones, como las relativas a incumplimientos de normas internas de la organización o al control de riesgos penales o de incumplimientos normativos.

III.- ÁMBITO PERSONAL DE APLICACIÓN DEL SISTEMA INTERNO DE INFORMACIÓN DEL CENIEH.

Tendrán acceso al sistema, a través del canal interno y a los efectos previstos en el apartado anterior, los informantes personas físicas que hayan obtenido información sobre infracciones en su contexto laboral o profesional, comprendiendo en todo caso:

a) las personas que tengan la condición de empleados o trabajadores por cuenta ajena;

b) los autónomos;

c) los partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de la organización, incluidos los miembros no ejecutivos;

d) cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

e) También, quienes comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral o estatutaria ya finalizada, voluntarios, becarios,

trabajadores en periodos de formación con independencia de que perciban o no una remuneración, así como a aquellos cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.

IV.- COMPETENCIAS Y RESPONSABILIDADES DEL CONSEJO RECTOR DEL CENIEH EN RELACIÓN AL SISTEMA INTERNO DE INFORMACIÓN.

El Consejo Rector del CENIEH, como máximo órgano de gobierno del CENIEH, es el responsable de la implantación del sistema interno de información, previa consulta con la representación legal de las personas trabajadoras, y tendrá la condición de responsable del tratamiento de los datos personales de conformidad con lo dispuesto en la normativa sobre protección de datos personales. Entre otras competencias, corresponde al Consejo Rector:

1ª.- Aprobar la política del CENIEH en materia de sistema interno de información y defensa del informante y que sea debidamente publicitada en el seno de la entidad.

2ª.- Aprobar el procedimiento de gestión de las informaciones recibidas.

3ª.- Designar un responsable del dicho sistema interno de información.

V.- PRINCIPIOS GENERALES DEL SISTEMA DE INFORMACIÓN DEL CENIEH.

Son principios generales del sistema interno de información del CENIEH, los siguientes:

1. Facilitar el acceso y uso del canal interno de información a los informantes personas físicas que hayan obtenido información sobre infracciones en su contexto laboral o profesional.

2. Estar diseñado, establecido y gestionado de una forma segura, de modo que se garantice la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la protección de datos, impidiendo el acceso de personal no autorizado.

3. Permitir la presentación de comunicaciones por escrito o verbalmente, o de ambos modos.

4. Integrar los distintos canales internos de información que, en su caso, pudieran establecerse dentro del CENIEH.

5. Garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva dentro del CENIEH con el objetivo de que el primero en conocer la posible irregularidad sea la propia entidad.

6. Ser independiente y aparecer diferenciado respecto de los sistemas internos de información de otras entidades u organismos.

7. Contar con un responsable del sistema.

8. Contar con una política o estrategia que enuncie los principios generales en materia de sistemas interno de información y defensa del informante y que sea debidamente publicitada en el seno del CENIEH.

9. Contar con un procedimiento de gestión de las informaciones recibidas para que el sistema interno de información y los canales internos de información existentes cumplan con los requisitos establecidos en la Ley. En particular, el procedimiento responderá al contenido mínimo y principios siguientes:

a) Identificar el canal o canales internos de información que integran el sistema.

b) Incluir 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.

c) Enviar al informante acuse de recibo de la comunicación en el plazo de siete días naturales siguientes a su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.

d) Determinar el 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, este podrá extenderse hasta un máximo de otros tres meses adicionales.

e) Prever la posibilidad de mantener la comunicación con el informante y, si se considera necesario, de solicitar a la persona informante información adicional.

f) Establecer el 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.

g) Garantizar 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.

h) Exigir el respeto a la presunción de inocencia y al honor de las personas afectadas.

i) Respetar las disposiciones sobre protección de datos personales de acuerdo a lo previsto en la Ley.

j) Remitir 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.

10. Establecer las garantías para la protección de los informantes en el ámbito del CENIEH, respetando, en todo caso, lo dispuesto en el procedimiento de gestión de informaciones.

VI.- REGISTRO DE INFORMACIONES.

1. El CENIEH contará 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.

Este registro 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.

2. Los datos personales relativos a las informaciones recibidas y a las investigaciones internas a que se refiere el punto anterior solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con la Ley. En ningún caso podrán conservarse los datos por un período superior a diez años.

VII.- MEDIDAS DE PROTECCIÓN AL INFORMANTE EN EL CENIEH.

Estas medias de protección del informante también se aplicarán, en su caso, a:

a) específicamente a los representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante,

b) personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso,

c) personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante, y

d) 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.

1. CONDICIONES DE PROTECCIÓN.

1. Las personas que comuniquen o revelen infracciones previstas en la Ley tendrán derecho a protección siempre que concurran las circunstancias siguientes:

a) tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación o revelación, aun cuando no aporten pruebas concluyentes, y que la citada información entra dentro del ámbito de aplicación de la Ley,

b la comunicación o revelación se haya realizado conforme a los requerimientos previstos en la Ley.

2. Quedan expresamente excluidos de protección aquellas personas que comuniquen o revelen:

a) Informaciones contenidas en comunicaciones que hayan sido inadmitidas por algún canal interno de información o por alguna de las causas previstas en el procedimiento de gestión de las informaciones recibidas.

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

c) Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores.

d) Informaciones que se refieran a acciones u omisiones no comprendidas en el apartado II de esta política.

3. Las personas que hayan comunicado o revelado públicamente información sobre acciones u omisiones a que se refiere la Ley de forma anónima pero que posteriormente hayan sido identificadas y cumplan las condiciones previstas en la Ley, tendrán derecho a protección.

4. Las personas que informen ante las instituciones, órganos u organismos pertinentes de la Unión Europea infracciones que entren en el ámbito de aplicación de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, tendrán derecho a protección en las mismas condiciones que una persona que haya informado por canales internos.

2. PROHIBICIÓN DE REPRESALIAS.

1. Se prohíben expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación conforme a lo previsto en la Ley.

2. Se entiende por represalia cualesquiera actos u omisiones que estén prohibidos 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, solo por su condición de informantes, o por haber realizado una revelación pública.

3. A los efectos de lo previsto en la Ley, y a título enunciativo, se consideran represalias las que se adopten en forma de:

a) Suspensión del contrato de trabajo, despido o extinción de la relación laboral o estatutaria, incluyendo la no renovación o la terminación anticipada de un contrato de trabajo temporal una vez superado el período de prueba, o terminación anticipada o anulación de contratos de bienes o servicios, imposición de cualquier medida disciplinaria, degradación o denegación de ascensos y cualquier otra modificación sustancial de las condiciones de trabajo y

la no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido; salvo que estas medidas se llevaran a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral o reguladora del estatuto del empleado público correspondiente, por circunstancias, hechos o infracciones acreditadas, y ajenas a la presentación de la comunicación.

b) Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.

c) Evaluación o referencias negativas respecto al desempeño laboral o profesional.

d) Inclusión en listas negras o difusión de información en un determinado ámbito sectorial, que dificulten o impidan el acceso al empleo o la contratación de obras o servicios.

e) Denegación o anulación de una licencia o permiso.

f) Denegación de formación.

g) Discriminación, o trato desfavorable o injusto.

3. MEDIDAS DE PROTECCIÓN FRENTE A REPRESALIAS.

1. No se considerará que las personas que comuniquen información sobre las acciones u omisiones recogidas en la Ley o que hagan una revelación pública de conformidad con la Ley hayan infringido ninguna restricción de revelación de información, y aquellas no incurrirán en responsabilidad de ningún tipo en relación con dicha comunicación o revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública de dicha información era necesaria para revelar una acción u omisión en virtud de la Ley. Esta medida no afectará a las responsabilidades de carácter penal.

Lo previsto en el párrafo anterior se extiende a la comunicación de informaciones realizadas por los representantes de las personas trabajadoras, aunque se encuentren sometidas a obligaciones legales de sigilo o de no revelar información reservada. Todo ello sin perjuicio de las normas específicas de protección aplicables conforme a la normativa laboral.

2. Los informantes no incurrirán en responsabilidad respecto de la adquisición o el acceso a la información que es comunicada o revelada públicamente, siempre que dicha adquisición o acceso no constituya un delito.

3. Cualquier otra posible responsabilidad de los informantes derivada de actos u omisiones que no estén relacionados con la comunicación o la revelación pública o que no sean necesarios para revelar una infracción en virtud de esta ley será exigible conforme a la normativa aplicable.

4. MEDIDAS PARA LA PROTECCIÓN D LAS PERSONAS AFECTADAS

Durante la tramitación del expediente las personas afectadas por la comunicación tendrán derecho a la presunción de inocencia, al derecho de defensa y al derecho de acceso al expediente

en los términos regulados en esta ley, así como a la misma protección establecida para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

5. SUPUESTOS DE EXENCIÓN Y ATENUACIÓN DE LA SANCIÓN

1. Cuando una persona que hubiera participado en la comisión de la infracción administrativa objeto de la información sea la que informe de su existencia mediante la presentación de la información y siempre que la misma hubiera sido presentada con anterioridad a que hubiera sido notificada la incoación del procedimiento de investigación o sancionador, el órgano competente para resolver el procedimiento, mediante resolución motivada, podrá eximirle del cumplimiento de la sanción administrativa que le correspondiera siempre que resulten acreditados en el expediente los siguientes extremos:

a) Haber cesado en la comisión de la infracción en el momento de presentación de la comunicación o revelación e identificado, en su caso, al resto de las personas que hayan participado o favorecido aquella.

b) Haber cooperado plena, continua y diligentemente a lo largo de todo el procedimiento de investigación.

c) Haber facilitado información veraz y relevante, medios de prueba o datos significativos para la acreditación de los hechos investigados, sin que haya procedido a la destrucción de estos o a su ocultación, ni haya revelado a terceros, directa o indirectamente su contenido.

d) Haber procedido a la reparación del daño causado que le sea imputable.

2. Cuando estos requisitos no se cumplan en su totalidad, incluida la reparación parcial del daño, quedará a criterio de la autoridad competente, previa valoración del grado de contribución a la resolución del expediente, la posibilidad de atenuar la sanción que habría correspondido a la infracción cometida, siempre que el informante o autor de la revelación no haya sido sancionado anteriormente por hechos de la misma naturaleza que dieron origen al inicio del procedimiento.

3. La atenuación de la sanción podrá extenderse al resto de los participantes en la comisión de la infracción, en función del grado de colaboración activa en el esclarecimiento de los hechos, identificación de otros participantes y reparación o minoración del daño causado, apreciado por el órgano encargado de la resolución.

VIII.- PROTECCIÓN DE DATOS PERSONALES

Según lo dispuesto en la normativa de protección de datos de carácter personal, aquellos que se reciban a través del canal interno de información serán tratados e incorporados en una actividad de tratamiento, cuya finalidad es la correcta gestión del canal interno de información en el CENIEH. La legitimación para el tratamiento de sus datos, por tanto, es una obligación legal

impuesta por 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.

Es probable, que, a la hora de emitir una comunicación, sean revelados datos especialmente protegidos, como, por ejemplo, datos relativos a su salud, vida y orientación sexual, que revelen su origen étnico o racial o que revelen una situación de acoso. En tal caso, la licitud para el tratamiento de los mismos responderá a los artículos 9.2.b y 9.2.h del Reglamento (UE) 2016/679, de Protección de Datos Personales y garantía de los derechos digitales, es decir, aquella relativa al cumplimiento de obligaciones legales y que el tratamiento es necesario por razones de interés público esencial.

El tratamiento de datos personales derivado de una revelación pública se presumirá amparado en lo dispuesto en los artículos 6.1.e) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 11 de la Ley Orgánica 7/2021, de 26 de mayo, en tanto esta responde al cumplimiento de una misión realizada en interés público.

Además, en caso de que sea comunicada una dirección de correo electrónico, número de teléfono u otro medio para ponernos en contacto con el informante a la hora de gestionar la comunicación emitida, la legitimación para notificarle cuantas circunstancias y requerimientos sean necesarios para la correcta marcha del proceso de investigación responderá también a una obligación legal aplicable al responsable del sistema.

Los datos proporcionados se conservarán durante el tiempo necesario para cumplir con las exigencias legales y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos.

Dentro del ámbito de la entidad, tan solo tendrán acceso a los datos que proporcione, y siempre que responda a una necesidad para el desarrollo de la gestión de las comunicaciones recibidas, el responsable del sistema, el responsable de recursos humanos u órgano competente designado, el responsable de servicios jurídicos y el delegado de protección de datos. No se cederán datos a terceros, salvo obligación legal, en su caso, a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa o cuando esta comunicación sea necesaria para la correcta gestión de las comunicaciones emitidas a través del canal interno de información a encargados de tratamiento debidamente designados.

Los datos personales recibidos se tratarán conforme a las máximas de confidencialidad, seguridad de la Información y respeto, en todo momento, al anonimato del informante.

---------- ------ 0 ----------

La presente política del CENIEH en materia de sistema interno de información y defensa del informante ha sido aprobada por el Consejo Rector del CENIEH en reunión celebrada el 19/07/23