SISTEMA DE GESTIÓN DE COMPLIANCE PENAL

ANEXO 11

POLÍTICA GENERAL DEL SISTEMA INTERNO DE INFORMACIÓN Y DEFENSA DEL INFORMANTE

Y PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES RECIBIDAS E INVESTIGACIONES INTERNAS

-CANAL ÉTICO Y/O DE DENUNCIAS-

-CANALES INTERNOS DE COMUNICACIÓN DE INFRACCIONES / CONSULTAS-

SISTEMA GESTIÓN COMPLIANCE PENAL

POLÍTICA DE USO DE LOS CANALES INTERNOS DE COMUNICACIÓN / INFORMACIÓN DE INFRACCIONES ("SISTEMA INTERNO DE INFORMACIÓN")

CONTENIDO

1. INTRODUCCIÓN, OBJETIVO Y DEFINICIONES

1.1 La legislación actual (art 31 bis del Código Penal), dentro del esquema de establecer una verdadera cultura corporativa ética y de cumplimiento, así como de un modelo o Sistema de Gestión de Compliance Penal (en adelante también SGCP) para la prevención, detección y reacción ante delitos, establece, como uno de los requisitos del modelo la obligación de informar de posibles riesgos e incumplimientos al órgano encargado de vigilar su funcionamiento y observancia, el Órgano de Compliance Penal. Consideramos el Sistema Interno de Información (Canal de Denuncias Interno) una vía adecuada y eficaz para dar cumplimiento a este requisito.

1.2 Por tanto, el órgano de gobierno de ENSOTRANS MARESME, S.L., (en adelante también ENSOTRANS o la ORGANIZACIÓN), por tanto, en el desarrollo de su compromiso con los principios de buena gobernanza, el Código Ético y de Conducta y la Política de Compliance Penal, como estándares de comportamiento exigidos de obligado cumplimiento, y en general con el Sistema de Gestión de Compliance Penal, así como con el cumplimiento normativo, elabora la presente Política, habilitando un Sistema Interno de Información o Canal de Denuncias Interno, que, entre otros extremos:

- Enuncia los principios generales en materia de Sistemas interno de información y defensa del informante.
- Es debidamente publicitada en el seno de la Organización.
- Contiene el procedimiento de gestión de informaciones.
- Integra los distintos canales internos de información establecidos dentro de la Organización.
- Garantiza que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la Organización con el objetivo de que el primero en conocer la posible irregularidad sea la propia Organización.
- Es independiente y aparece diferenciado respecto de los sistemas internos de información de otras entidades u organismos.
- Establece garantías para la protección de los informantes en el ámbito de la propia Organización.

1.3 No obstante, ENSOTRANS MARESME, S.L. no se halla obligado a disponer de un Sistema Interno de Información de acuerdo al art. 10.1 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, por ser empresas en el ámbito privado que no tienen contratados cincuenta o más trabajadores, adopta como referencia las disposiciones de la referida Ley 2/2023. Ello, de acuerdo con lo establecido en el Preámbulo y el artículo 10.2 de la indicada Ley 2/2023:

> *"Preámbulo: En el ámbito privado, siguiendo la previsión de la Directiva, estarán obligadas a configurar un Sistema interno de información todas aquellas empresas que tengan más de cincuenta trabajadores".*
>
> *Artículo 10. Entidades obligadas del sector privado. 1. Estarán obligadas a disponer un Sistema interno de información en los términos previstos en esta ley: a) Las personas físicas o jurídicas del sector privado que tengan contratados cincuenta o más trabajadores.*

1.4 La presente Política tiene por objeto regular el Sistema Interno de Información de ENSOTRANS MARESME, S.L., y en particular:

- Habilitar e implementar el Sistema Interno de Información, a fin de prevenir y detectar conductas irregulares, ilícitas, delictivas o que atenten contra los derechos humanos.

- Dar cumplimiento al requisito establecido en el art. 31 bis 5.4 del Código Penal español de informar de posibles riesgos e incumplimientos al órgano encargado de vigilar su funcionamiento y observancia, el Órgano de Compliance Penal; en caso de resultar aplicables a la Ley 2/2023 así como de la Directiva Europea 1937/2019.
- Fomentar la participación y comunicación entre la Entidad y sus grupos de interés.
- Fomentar una cultura de ética e integridad, buena comunicación y responsabilidad social empresarial en la Organización, en virtud de la cual se considera que los informantes o denunciantes contribuyen de manera significativa a la autocorrección y la excelencia dentro de la Organización.
- Fortalecer la cultura de la información, de la infraestructura de integridad de la Entidad, y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público.
- Proteger a empleados y terceros de actos deshonestos o discriminatorios.
- Prevenir y detectar en una etapa temprana posibles incumplimientos normativos que se estén produciendo en la organización con la finalidad de subsanarlos, así como actos que puedan constituir una infracción penal de acuerdo con el principio de tolerancia cero ante este tipo de conductas dentro de la Entidad.
- Definir el procedimiento de comunicación y gestión de las denuncias recibidas, así como las garantías y derechos de las partes.
- Proteger adecuadamente a las personas que en un contexto laboral o profesional detecten infracciones penales o administrativas graves o muy graves y las comuniquen a través de los canales previstos en la presente Política, frente a las represalias que pudieran sufrir de muy diversas formas.
- Para la implementación del presente Sistema Interno de Información se realizará, en su caso, consulta previa a los representantes de los trabajadores.

1.5 El Sistema Interno de Información, además de servir para descubrir e investigar posibles infracciones o irregularidades, es una herramienta imprescindible para que el Código Ético y de conducta y al Política de Compliance Penal y sus valores cobren total vigencia y posibilite la mejora continua de los protocolos y políticas de prevención, normas de transparencia y demás normativa interna.

1.6 Las personas que trabajan para una organización, o están en contacto con ella y acceden a la información a través de sus actividades laborales relacionadas con la organización (socios o accionistas, miembros del órgano de administración, personas empleadas en concepto amplio, direcciones o responsables de área o departamento, voluntarios, trabajadores en prácticas, ex-trabajadores, candidatos, proveedores, consultores, profesionales autónomos, contratistas, subcontratistas, agentes, etc.) son a menudo las primeras en tener conocimiento de amenazas o perjuicios para el interés público que surgen en ese contexto, suelen encontrarse en una posición privilegiada, y por ello desempeñan un papel clave a la hora de descubrir y prevenir infracciones y de proteger el bienestar de la Organización, lo que permite a su vez detectar, investigar y enjuiciar de manera efectiva las infracciones, mejorando así la transparencia y la rendición de cuentas.

1.7 Como consecuencia de la firme voluntad de ser una Organización guiada por la ética y por los referidos valores corporativos, ENSOTRANS MARESME valora positivamente y anima a toda persona que tenga conocimiento o viva personalmente una situación que pueda considerarse ilícita o irregular y se encuentre dentro de las conductas denunciables de la presente Política, a informar inmediatamente mediante el canal establecido.
En el cumplimiento de su objetivo social, ENSOTRANS MARESME actuará respetando en todo momento la legalidad vigente y la aplicación de los principios y valores en todas las relaciones tanto internas como externas.

1.8 En este marco es esencial garantizar la protección efectiva frente a todo tipo de represalia, incluidas las amenazas de represalia y las tentativas de represalia, directa o indirecta, que se tome, aliente o tolere; ya sean directas contra denunciantes, así como frente aquellas que puedan tomarse indirectamente, incluso contra facilitadores, compañeros de trabajo, direcciones o responsables de área o departamento de la Organización, familiares del denunciante que también mantengan una relación laboral con la Organización, o los clientes o destinatarios de los servicios del denunciante, incluyendo asimismo acciones tomadas contra la entidad jurídica de la que el denunciante sea propietario, para la que trabaje o con organizaciones con las que esté relacionado o en contacto de otra forma en el contexto de sus actividades laborales.

1.9 La posición y reputación de la Organización es el resultado de muchos años de esfuerzo y trabajo y el comportamiento inadecuado de un sólo empleado puede potencialmente dañar nuestra imagen y reputación en un espacio temporal muy corto. Desde la Organización se debe prevenir y evitar de forma activa esta posibilidad.

1.10 El Sistema Interno de Información es una herramienta efectiva para detectar irregularidades que pasarían inadvertidas por otros controles, aunque precisan cumplir medidas técnicas y jurídicas que garanticen los derechos de los afectados

1.11 En consecuencia, la aprobación de la presente Política de Uso del Sistema Interno de Información y su implantación en la Organización tiene como objetivo constituir un mecanismo eficaz, para que, a través de la colaboración de todos, se puedan detectar irregularidades o incumplimientos que puedan poner en riesgo a la Organización, a los Miembros de la Organización, en especial las personas empleadas que en ella prestan sus servicios, a los Socios de Negocio (ver definición en punto 3.1.2) y a otros grupos de interés.

1.12 La implantación del sistema interno de denuncia tendrá lugar sin perjuicio de la actividad de control que seguirán ejerciendo aquellos departamentos de la Organización con competencia en materias relacionadas con el Sistema de Gestión de Compliace Penal y el cumplimiento de las normativas. Cuando a resultas de la actividad de estos departamentos se descubra una posible infracción del Código Ético y de Conducta y/o la Política de Compliance Penal se actuará de acuerdo con lo previsto en la presente Política de Uso.

1.13 Definiciones: A efectos aclaratorios, se efectúan las siguientes definiciones que permitirán conocer el alcance de la presente Política:

Organización: a efectos de la presente Política, y del resto del SGCP, la Organización a la que le resulta aplicable es la constituida por la persona jurídica: ENSOTRANS MARESME, S.L.

Miembros de la Organización:

(i) Integrantes del órgano de administración, miembros de la alta dirección, direcciones o responsables de área o departamento, apoderados, y personas autorizadas para tomar decisiones en nombre de la Órganización o que ostenten facultades de organización y control en ella, y a los accionistas en lo que resulte de aplicación.

(ii) Personas empleadas, personas empleadas temporales o bajo convenio de colaboración, voluntarios de la Organización, becarios, trabajadores en periodos de formación con independencia de que perciban o no una remuneración, y en general personas sometidas a la autoridad de las personas físicas mencionadas en el punto anterior que actúen bajo su supervisión, vigilancia y control.

Socios de Negocio: cualquier parte, salvo los Miembros de la Organización, con quien la Organización mantiene o prevé establecer algún tipo de relación de colaboración o de negocio. A modo enunciativo, pero no limitativo, se incluyen clientes, asesores externos, consultores, proveedores de bienes o servicios, contratistas, intermediarios e inversores, joint ventures, socios de joint ventures etc. El término "negocio" debe interpretarse en sentido amplio, refiriéndose a aquellas actividades que son fundamentales o beneficiosas para el propósito de la existencia de la Organización.

Partes interesadas o grupos de interés: cualquier persona u Organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad de la Organización.

Tercero: persona física o jurídica u órgano independiente de la Organización.

Sistema de Gestión de Compliance Penal (SGCP): conjunto de elementos de la Organización interrelacionados o que interactúan para concretar y medir de nivel de consecución de los objetivos del compliance penal, así como las políticas, procesos y procedimientos para lograr dichos objetivos.

Política de Compliance Penal: es el conjunto de disposiciones contenidas en dicho texto, y que constituyen la voluntad de la Organización según la expresa el Órgano de Administración, en relación a sus objetivos de compliance penal. La Política de Compliance Penal desarrolla lo establecido en el Código Ético y de Conducta, principalmente sus apartados 5 y 6, y, por consiguiente, enlaza con sus valores éticos, ratificando la firme voluntad de la Organización por mantener una conducta respetuosa tanto con las normas como con los estándares éticos y fijando, para ello, su marco de principios de cumplimiento en materia penal.

2. NORMATIVA APLICABLE Y DOCUMENTACIÓN RELACIONADA

2.1 NORMATIVA EXTERNA

- Código Penal español.
- Ley de Enjuiciamiento Criminal.
- Circulares del Ministerio Fiscal.
- Ley 2/2023 reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción por la que se transpone la 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.
- Normativa relativa a protección de datos personales (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales).
- Regulación laboral (Convenios Colectivos y Estatuto de los Trabajadores).
- Otras normativas que resulte de aplicación.

2.1. NORMATIVA INTERNA

- Código Ético y de Conducta y la Política de Compliance Penal de la Organización.
- Sistema de Gestión de Compliance Penal - política de prevención, detección y reacción frente a riesgos penales de la Organización -.
- Políticas, protocolos, procedimientos, manuales, normas o controles internos de la Organización en relación a riesgos penales y/o incumplimientos del Código Ético y de Conducta y Política de Compliance Penal: Protocolo de Acoso, etc.

3. PRINCIPIOS / REQUISITOS GENERALES DE LOS CANALES INTERNOS DE COMUNICACIÓN / INFORMACIÓN DE INFRACCIONES ("SISTEMA INTERNO DE INFORMACIÓN")

3.1 Los referidos canales ("Sistema interno de Información") responden, entre otros, a los siguientes principios generales y requisitos:

3.1.1 Principios generales, que deben regir el funcionamiento de cualquier Sistema Interno de Información:

a) Accesibilidad: Los canales de comunicación son claros, públicos y de fácil acceso a personas empleadas y terceros que deseen interponer una comunicación en los términos previstos en la presente Política.

b) Buena fe: Se considerará que el denunciante actúa de buena fe cuando su denuncia se realice conforme a lo dispuesto en la presente Política y esté basada en hechos o indicios de los que razonablemente pueda desprenderse la realización de un comportamiento irregular, ilícito, delictivo o contrario a los principios y valores de la entidad o a las normas de actuación recogidas en nuestros Código Ético y de Conducta y Política de Compliance Penal y el resto de políticas aprobadas, por el Órgano de Gobierno.

Se considerará que la denuncia es de buena fe cuando se realice sin ánimo de venganza, de acosar moralmente, de causar un perjuicio laboral o profesional, o de lesionar el honor de la persona denunciada o de un tercero. Se considera que el denunciante no actúa de buena fe cuando el autor de la denuncia es consciente de la falsedad de los hechos, o actúa con manifiesto desprecio a la verdad, o con la intención de venganza, o de perjudicar a ENSOTRANS MARESME o de acosar a la persona denunciada, o de lesionar su honor, o de perjudicarle laboral, profesional o personalmente.

Si se demuestra que la denuncia se ha realizado de mala fe, no actuará la protección al denunciante y se podrán aplicar medidas tanto disciplinarias como penales.

c) Protección al denunciante y principio de no represalia: Ante cualquier denuncia que se pueda realizar, independientemente del canal utilizado, quedará garantizada la protección de los derechos del denunciante, posibles víctimas, testigos y, en su caso, denunciados, de conformidad con el procedimiento establecido.
Igualmente, ENSOTRANS MARESME se compromete a garantizar la protección del denunciante frente a represalias de cualquier naturaleza, directas o indirectas, incluidas las amenazas de represalia y las tentativas de represalia.

d) Confidencialidad: La identidad de la persona que realice la comunicación tendrá la consideración de información confidencial y no podrá ser comunicada ni revelada sin su consentimiento. No obstante, los datos de las personas que efectúen la comunicación podrán ser facilitados tanto a las autoridades administrativas como a las judiciales siempre que fueran requeridos como consecuencia de cualquier procedimiento judicial derivado del objeto de la denuncia. Dicha cesión de los datos a las autoridades administrativas o judiciales se realizará siempre dando pleno cumplimiento a la legislación vigente sobre protección de datos de carácter personal.

e) Objetividad e imparcialidad: Una vez recibida una denuncia, se garantizará el derecho a la intimidad, a la defensa y a la presunción de inocencia de las personas objeto de la misma. La persona Responsable del Sistema de ENSOTRANS MARESME es la persona que, por nombramiento del Órgano de Administración, está encargada de coordinar e impulsar el tramitación y resolución de las diferentes denuncias recibidas a través del Sistema Interno de Información, de manera objetiva y en base a criterios de imparcialidad y respeto de los principios y derechos contenidos en la presente Política.

f) Transparencia: El Sistema Interno de Información de ENSOTRANS MARESME es una herramienta de transparencia que favorece la confianza de las personas y los grupos de interés en los mecanismos con los que cuenta la organización para garantizar el cumplimiento de la legalidad y de los principios y valores recogidos en el Código Ético y de Conducta, Política de Compliance Penal y demás normativa interna.

3.1.2 Requisitos.

a) Son implantados por acuerdo o decisión del Órgano de Gobierno, previa consulta, en su caso, con la representación legal de las personas trabajadoras, y ENSOTRANS MARESME tendrá la condición de responsable del tratamiento de los datos personales de conformidad con lo dispuesto en la normativa sobre protección de datos personales.
b) Están diseñados, establecidos y gestionados 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.
c) Permiten la realización de comunicaciones de manera confidencial, e incluso la presentación y posterior tramitación de comunicaciones anónimas.
d) Permiten la presentación de comunicaciones por escrito y verbalmente.
e) Se integran los distintos canales internos de información de la Organización.
f) Garantizan que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la correspondiente entidad con el objetivo de que el primero en conocer la posible irregularidad sea la propia Organización.
g) Son independientes y aparecer diferenciados respecto de los sistemas internos de información de otras entidades.
h) Cuentan con un Responsable del Sistema.
i) Se cuenta con una Política que enuncia los principios generales en materia de Sistemas interno de información y defensa del informante, y con un procedimiento de gestión de las informaciones recibidas, debidamente publicitados en el seno de la Organización.
j) Establece garantías para la protección de los informantes en el ámbito de la propia Organización.
k) Se facilitará asesoramiento sobre el SGCP a aquellas personas que planteen dudas o inquietudes a través de los referidos canales de comunicación establecidos.
l) Garantiza que los Miembros de la Organización conocen su existencia y los procedimientos que regulan su funcionamiento.
m) Fomentará el uso de los canales de comunicación entre los Miembros de la Organización.
n) Exigencia del respeto a la presunción de inocencia y al honor de las personas afectadas.
o) Respeto de las disposiciones sobre protección de datos personales.
p) Prohíbe cualquier tipo de represalia y garantiza que la Organización tomará todas las medidas necesarias para proteger a los Miembros de la Organización o terceros que realicen comunicaciones de buena fe y sobre la base de indicios razonables.

Se prohíben expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas informantes / denunciantes.

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.

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, 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.

La referida prohibición de actos constitutivos de represalia incluye además del propio denunciante / informante a:

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

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

c) 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.

4. ALCANCE SUBJETIVO

4.1 La presente Política será de aplicación a los siguientes informantes:

a) Personas empleadas (trabajadoras por cuenta ajena) de las sociedades de ENSOTRANS MARESME.
b) Los accionistas y personas pertenecientes al órgano de administración, dirección o supervisión de la Entidad, incluidos los miembros no ejecutivos, así como los voluntarios y trabajadores en prácticas remuneradas o no; personas que ya no tengan relación con la organización por haber expirado ésta, becarios y personal en formación.
c) En general, todos los Miembros de la Organización de acuerdo con la definición establecida en el punto 1.13 de la presente Política.

d) Socios de Negocio de acuerdo con la definición establecida en el punto 1.13 de la presente Política, incluyendo autónomos y cualquier persona que trabaje bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

e) Informantes que comuniquen o revelen públicamente información sobre infracciones obtenidas en el marco de una relación laboral ya finalizada.

f) Informantes cuya relación laboral todavía no haya comenzado, si la infracción se obtiene durante el proceso de selección o negociación precontractual.

g) Todos aquellos que de forma directa o indirecta intervengan en el procedimiento y puedan ser represaliados por ello (asesores del informante, representantes, etc.).

h) En relación a las medidas de protección del informante también se aplicarán, en su caso, a:

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

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

(iii) 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

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

4.2 Todos los Miembros de la Organización deberán comunicar, a través del Sistema interno de Información cualquier irregularidad o incumplimiento de los que tengan conocimiento y que estén incluidos en su alcance objetivo.

4.3 Además, desde la Organización se informará, en el plan de implantación del SGCP, a todos sus Socios de Negocio, y en general a las demás partes interesadas o grupos de interés de la existencia y contenido de su Código Ético y de Conducta, Política de Compliance Penal, y su Sistema Interno de Información, a través de la web corporativa, que, en la medida de lo posible, también les resultará de aplicación.

En consecuencia, la Organización promoverá e incentivará entre sus Socios de Negocio y demás partes interesadas o grupos de interés, la adopción de pautas de comportamiento consistentes con las que se definen en el Código y la Política referidos, y en su caso, podrá solicitarles que formalicen su compromiso con el cumplimiento del Código Ético y de Conducta, la Política de Compliance Penal y con el deber de denuncia a través del Sistema Interno de Información.

4.4 Sin perjuicio de las personas que tengan el deber de denunciar, cualquier persona podrá comunicar a través del Sistema Interno de Información cualquier infracción, irregularidad o incumplimiento de los que tengan conocimiento que estén incluidos en su alcance objetivo.

5. ALCANCE OBJETIVO

5.1 El alcance de aplicación objetivo se extiende a los siguientes incumplimientos o irregularidades:

a) Conductas (acciones u omisiones) tipificadas en el Código Penal español, que puedan ser constitutivas de infracción penal, y los delitos previstos en otras leyes especiales que se detallan en el ANEXO I, que apliquen en cada momento a la Organización.

b) Acciones u omisiones que puedan ser constitutivas de infracción administrativa grave o muy grave, incluyendo siempre las que afecten a un quebranto económico a la Hacienda Pública y a la Seguridad Social.

c) Cualesquiera acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea siempre que:

(i) entren dentro del ámbito de aplicación de los actos de la Unión Europea enumerados en el anexo de la 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, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno:

- 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

(ii) afecten a los intereses financieros de la Unión Europea tal y como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE) o

(iii) Incidan en el mercado interior, tal y como se contempla en el artículo 26, apartado 2 del TFUE, 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.

d) Infracciones del Derecho laboral en materia de seguridad y salud en el trabajo.

e) Todos aquellos incumplimientos o conductas contrarias a los principios, valores y normas de conducta establecidas en el Código Ético y de Conducta y/o Política de Compliance Penal de la Organización, y en general al Sistema de Gestión de Compliance Penal (SGCP) de la Organización -política de prevención, detección, gestión y reacción frente a riesgos penales-.

f) Todas aquellos incumplimientos o conductas contrarias Políticas, protocolos, procedimientos, manuales, normas o controles internos de la Organización con relación a riesgos penales y/o incumplimientos del Código Ético y de Conducta.

g) Cualquier acto de discriminación por cualquier razón, acoso ya sea de tipo laboral (mobbing) o sexual o por razón de sexo en el seno de la Organización y hacia terceros.

h) Y, en general, cualesquiera situaciones o hechos que requieran la atención del Órgano de Compliance Penal de la Organización.

5.2 Las informaciones a comunicar podrán incluir las sospechas razonables, sobre infracciones reales o potenciales, que se hayan producido o que muy probablemente puedan producirse en la Organización, en la que trabaje, haya trabajado el denunciante o hubiera estado en contacto con motivo de su trabajo, y sobre intentos de ocultar tales infracciones.

5.3 Asimismo, el Sistema Interno de Información constituye una vía para plantear inquietudes, dudas, consultas o sugerencia de mejora relacionadas con Código Ético y de Conducta, la Política de Compliance Penal, y en general, el Sistema de Gestión de Compliance Penal, o con las propias actividades de la Organización que puedan suscitar temor a un incumplimiento.

5.4 Con independencia de la posibilidad de recibir otras denuncias, quejas y/o reclamaciones de otros ámbitos normativos, única y exclusivamente quedarán amparadas bajo las medidas de protección que se establecen en la Ley 2/2023 aquellas comunicaciones recogidas en el artículo 2 de misma.

5.5 La presente Política se entiende sin perjuicio de las normas de procedimiento recogidas en el Protocolo para la prevención, detección y actuación frente a conductas de acoso, agresión sexual, y/o actos discriminatorios (acoso laboral, moral o psicológico, acoso sexual, acoso por razón de sexo, de identidad sexual y/o de género, agresión sexual, violencia digital o ciberacoso, violencia física, y/o actos discriminatorios), y en todos aquellos que pudieran acordarse en un futuro.

La gestión interna de las informaciones que sean objeto del citado protocolo se tramitará de conformidad con lo dispuesto en él, que en todo caso contará con las garantías y plazos previstos en la Ley 2/2023. Aquellas otras conductas que tengan un procedimiento específico establecido al efecto se regirán por el mismo. En todo lo no previsto en el Procedimiento, regirá la Ley 2/2023.

La unidad correspondiente competente será la responsable de su resolución, de lo que informará al órgano Responsable del Sistema de Información, y llevará a cabo las comunicaciones pertinentes.

6. CANALES INTERNOS HABILITADOS DE COMUNICACIÓN / INFORMACIÓN DE INFRACCIONES ("SISTEMA INTERNO DE INFORMACIÓN") PARA REALIZAR COMUNICACIONES DE UNA DENUNCIA

6.1 Los denunciantes podrán efectuar una comunicación de la denuncia por cualquiera de los siguientes canales habilitados:

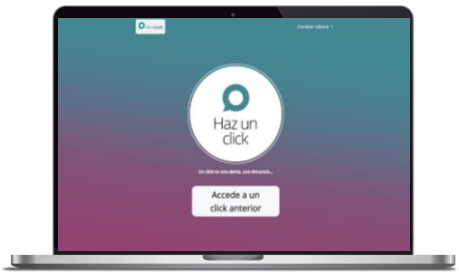
a) De forma escrita, la comunicación / denuncia deberá realizarse:

- Como canales principales para la recepción de informaciones, ENSOTRANS MARESME pone a disposición de los denunciantes, para facilitar su preceptiva accesibilidad en la página web corporativa, el acceso a una plataforma (mediante app o web) proveída por una empresa tecnológica especializada, que cuenta con medidas técnicas adecuadas para garantizar la confidencialidad y la seguridad de la información, así como el anonimato cuando se opte por esta modalidad de comunicación.
  Existen las siguientes dos opciones (mediante la app Co-Resol o mediante página web), que permiten realizar la comunicación tanto de forma nominal y confidencial como anónima, y en el primer caso se reserva la identidad del informante:

OPCIÓN 1: Enviar una notificación a través de APP móvil (co-resol):

1. Descárgate la app co-resol, aceptando las notificaciones. Es gratuita y está disponible en la App Store y en Google Play.
2. Pulsa el botón "Haz un click" y a continuación introduce el siguiente código: ENSOTRANS
3. Selecciona el botón del canal.
4. Escribe tu mensaje siendo lo más específico posible. Puedes adjuntar tanto imágenes como documentación.
5. Identifícate o selecciona la opción de anonimato. En cualquiera de los casos, debes aceptar la Política de Privacidad.
6. Una vez hayas efectuado estos pasos, recibirás un mensaje como acuse de recibo de tu click.
7. La comunicación para el seguimiento del click se realizará mediante un chat seguro (podrás acceder al mismo desde el botón de chat de la pantalla de inicio de la app) hasta el cierre del mismo.

OPCIÓN 2: Enviar una notificación a través de una página web



Puedes acceder a ella a través de este enlace:

https://co-resol.bcnresol.com/webclick

1. Pulsa el botón "Haz un click" y a continuación introduce el siguiente código: **ENSOTRANS**
2. Selecciona el botón del canal.
3. Escribe tu mensaje siendo lo más específico posible. Puedes adjuntar tanto imágenes como documentación.
4. Identifícate o selecciona la opción de anonimato. En cualquiera de los casos, debes aceptar la Política de Privacidad.
5. En este caso, recibirás un código identificador y una contraseña únicos que deberás guardar para mantener la comunicación, a través de un chat seguro, sobre el estado de tu click.
6. Cada vez que quieras saber si tienes mensaje nuevo en el chat o quieras aportar más información, para asegurar la confidencialidad, debes introducir este código y contraseña en la página de inicio, en el botón "Acceder a un click anterior".

Aspectos sobre el uso y manejo del canal

Te informamos que al canal permite tanto realizar comunicaciones por primera vez como acceder a comunicaciones previas realizadas para poder hacer seguimiento de estas.

CO-RESOL (web) es una plataforma disponible las 24 horas del día, los 365 días del año.

El Canal (CO-RESOL) proporciona acuse de recibo automático y posibilita incorporar archivos de todo tipo (incluidos audios). Incorpora encriptación extremo a extremo y de los datos personales en bases de datos.

Da estricto cumplimiento de la Ley 2/2023 de protección a la persona informante y a la normativa vigente sobre protección de datos de carácter personal.

- Remitiendo un correo electrónico a la dirección de correo electrónico establecida compliance@ensotrans.com, o la que la sustituyera.

b) De forma presencial, en el domicilio social de ENSOTRANS MARESME, sito en C/ Remallaire, 15, local 1. 08302, Mataró. (Barcelona), a solicitud del informante, dentro del plazo máximo de siete días, ante el Comité de Ética y Cumplimiento.

Las comunicaciones verbales realizadas a través de reunión presencial se documentarán de alguna de las maneras siguientes, previo consentimiento del informante:

i. a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.
ii. mediante una grabación de la conversación en un formato seguro, duradero y accesible.

Sin perjuicio de los derechos que le corresponden de acuerdo con la normativa sobre protección de datos, se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

En su caso, se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo con lo que establece el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Realizada la comunicación se quedará registrada con un código de seguimiento por cada uno de los expedientes, que recibirán los informantes en el correo electrónico que indiquen en la comunicación.

c) Por excepción, cuando las conductas o situaciones que debieran ser objeto de comunicación afectasen personalmente a los integrantes del Comité de Gestión e Investigación de Informaciones las comunicaciones o denuncias deberán dirigirse al Órgano de Gobierno.

6.2 Al presentar la información, el informante podrá renunciar expresamente a la recepción de cualquier comunicación de actuaciones llevadas a cabo.

6.3. El Sistema Interno de Información Digital se encuentra en una base de datos segura y de acceso restringido a los usuarios exclusivamente designados.

6.4 Canal de comunicación en materia de prevención del acoso, recogido en el Protocolo para la prevención y actuación frente al acoso sexual y acoso por razón de sexo en el ámbito laboral (ver punto 5.5).

7. RESPONSABLE ("RESPONSABLE DEL SISTEMA") Y RÉGIMEN DE GESTIÓN (RECEPCIÓN DE LAS COMUNICACIONES) DE LOS CANALES INTERNOS DE COMUNICACIÓN / INFORMACIÓN DE INFRACCIONES ("SISTEMA INTERNO DE INFORMACIÓN")

7.1 Responsable del Sistema:

7.1.1 El Órgano de Gobierno designará la persona física u órgano colegiado responsable de la gestión de los referidos canales internos de comunicación /información ("Responsable del Sistema") y será el competente, asimismo, para su destitución o cese.

7.1.2 El Órgano de Gobierno nombra, de acuerdo a la referida Ley 2/2023, de 20 de febrero, al Responsable del Sistema conforme a los siguientes requisitos y funciones:

- Debe ser un directivo
- Asume por delegación funciones legalmente asignadas
- Asume la gestión del Sistema Interno y responde de la tramitación diligente de las comunicaciones, ocupando una posición de garante respecto a la eficacia del Sistema.
- Debe 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.
- Deberá disponer de todos los medios personales y materiales necesarios.
- Ejercerá su cargo con independencia del órgano de administración.
- Funciones / Responsabilidades:
    - Gestionar y desarrollar con independencia y autonomía un Sistema interno eficaz, garantizando el cumplimiento efectivo de las obligaciones que le impone la Ley en esta materia y el correcto funcionamiento del Sistema.
    - Garantizar que las denuncias sean recibidas y procesadas adecuadamente.
    - Asegurarse de que los denunciantes reciban una respuesta oportuna y adecuada a sus denuncias.
    - Asegurar que los informes de denuncia sean registrados y archivados correctamente.
    - Colaborar con otras áreas de la organización para investigar y resolver los problemas que se reportan.
    - Responsabilizarse de la efectividad de la garantía de confidencialidad de los denunciantes en todos los niveles de la organización, y protegerlos contra posibles represalias.
    - Responsabilizarse de la tramitación diligente del Procedimiento de gestión de informaciones.
    - Responsabilizarse de la interlocución frente a las Autoridades Administrativas Independientes.
    - Las demás establecidas en la referida Ley 2/2023.

7.1.3 De conformidad a lo establecido en el punto anterior, el Órgano de Gobierno designa como persona Responsable de la gestión de los canales internos de comunicación/información ("Responsable del Sistema") de ENSOTRANS MARESME **a**

la Dirección del Departamento de Tráfico, Dña. Sonia Llobera Ruda, Directiva de la organización, que ejercerá su cargo con independencia del Órgano de Gobierno.

Como la dimensión de las actividades de la entidad no justifican ni permiten la existencia de un directivo exclusivo como persona designada por el Órgano de Gobierno como Responsable del Sistema, el desempeño ordinario de las funciones del puesto o cargo se compaginará con las de Responsable del Sistema, tratando en todo caso de evitar posibles situaciones de conflicto de interés

7.1.4 En el supuesto que el Órgano de Gobierno designase como Responsable del Sistema a un órgano colegiado, éste deberá delegar en uno de sus miembros las facultades de gestión de los canales internos de comunicación /información ("Sistema interno de Información") y de tramitación de expedientes de investigación; quien deberá ser un directivo de la Organización, que ejercerá su cargo con independencia del órgano de gobierno.

7.1.5 En caso de resultar obligatorio, el nombramiento y el cese de la persona física individualmente designada o de las personas integrantes del referido 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.

7.2 Gestión (recepción de las comunicaciones) de los canales internos de comunicación /información ("Sistema interno de Información")

7.2.1 La gestión de los referidos canales internos de comunicación /información establecidos ("Sistema interno de Información") podrá llevarse a cabo dentro de la propia Organización o mediante la gestión de un tercero externo, considerándose como gestión la recepción de informaciones.

7.2.2 ENSOTRANS MARESME opta por establecer un régimen de gestión (recepción de las comunicaciones) a través de un gestor externo. Con el ánimo de dotarlo de mayor profesionalidad y autonomía, y ofreciendo las garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones ENSOTRANS MARESME nombra a D. Fernando Cuatrecasas Cuatrecasas

7.2.3 La gestión por un tercero no podrá suponer un menoscabo de las garantías y requisitos establecidos en referidos canales internos de comunicación / información, ni una atribución de la responsabilidad sobre los mismos en persona distinta del Responsable del Sistema.

8. CANAL EXTERNO DE INFORMACIÓN

Comunicación a través del canal externo de información de la Autoridad Independiente de Protección del Informante, A.A.I.

Toda persona física podrá informar ante la Autoridad Independiente de Protección del Informante, A.A.I., o ante las autoridades u órganos autonómicos correspondientes, de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación 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, ya sea directamente o previa comunicación a través del Sistema Interno de Información de ENSOTRANS MARESME.

9. PUBLICIDAD DEL SISTEMA INTERNO DE INFORMACIÓN

9.1 ENSOTRANS MARESME proporcionará la información adecuada de forma clara y fácilmente accesible, sobre el uso del Sistema Interno de Información, así como sobre los principios esenciales del procedimiento de gestión, constando información en la página de la web corporativa, en una sección separada y fácilmente identificable.

10. REGISTRO DE INFORMACIONES / DENUNCIAS RECIBIDAS E INVESTIGACIONES INTERNAS REALIZADAS

10.1 La Organización 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 normativa vigente y el SGCP.

10.2 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.

10.3 Los datos personales relativos a las informaciones recibidas y a las investigaciones internas a que se refiere el apartado anterior solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir normativa vigente y el SGCP.

10.4 Los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados. Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

10.5 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 prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

En ningún caso podrán conservarse los datos por un período superior a diez años.

11. DATOS QUE SE DEBEN HACER CONSTAR EN LAS DENUNCIAS

11.1 En cualquier caso y, a los efectos de preservar el buen funcionamiento del procedimiento, la denuncia debe disponer de una serie de elementos para que pueda considerarse como tal y se produzca la posterior investigación en caso de que sea necesaria. La comunicación de la denuncia contendrá en la medida de lo posible, la siguiente información, salvo en el caso de denuncia anónima:

- Identificación del denunciante, salvo en caso de denuncia anónima.
- Fecha de la denuncia *(podrá ser campo automático en formulario web).*
- Función en la Organización o relación con la misma.
- Dirección o medio a efectos de contacto y notificaciones elegido por el denunciante (correo electrónico, correo postal, teléfono).
- Descripción del hecho denunciado, o comentario, consulta o sugerencia de mejora.
    - Con el fin de obtener la mejor información se recomienda que, en la medida de lo posible, describa en que consiste la conducta potencialmente irregular con descripción pormenorizada de los hechos que se denuncian, cuando y donde han ocurrido y las posibles personas implicadas o responsables (denunciadas), y otras informaciones relevantes.
    - Y si los conoce, los medios utilizados para llevar a cabo los hechos, cual es el área de actividad afectada, el posible impacto relevante en los procesos de trabajo de la Organización y si tiene o no impacto económico, y una cuantificación aproximada (en euros).
- Posibles personas implicadas o responsables (denunciadas).
- Fechas o periodos aproximados del riesgo, hecho, conducta, irregularidad o incumplimiento denunciado (requerido).
- En su caso, aportación de documentación soporte en la que se basa la denuncia o evidencias de los hechos de la denuncia de los que disponga.

11.2 En cualquier caso, la comunicación debe ser lo más descriptiva, concreta y detallada posible, facilitando de esta forma al receptor la identificación de la conducta potencialmente irregular y de la/las persona/s o departamento/s implicados. Los mensajes no deben contemplar palabras ofensivas.

11.3 Está permitida la presentación de comunicaciones anónimas en el Sistema Interno de Información (Canal Ético o de Denuncias) si, pese a la garantía de confidencialidad, el informante opta por el anonimato.
En este supuesto la tramitación del expediente puede quedar limitada ante la imposibilidad de contrastar la veracidad de la misma. En el caso de que el informante decida mantener el anonimato es conveniente manifestar el motivo para que se pueda tener en cuenta a la hora de tramitar la denuncia y realizar la investigación.

12. PROTECCIÓN DEL INFORMANTE Y DEL INVESTIGADO

En cualquier denuncia y procedimiento que se tramite se han de respetar los derechos y garantías de los denunciantes, víctimas y testigos. En este sentido, estarán protegidos frente a cualquier tipo de represalia, discriminación y penalización por motivo de las denuncias realizadas.

12.1 Derechos y garantías del informante

El informante tendrá las siguientes garantías en sus actuaciones ante ENSOTRANS MARESME y el Responsable del Sistema.

a) **Derecho a recibir información previa**: Previa interposición de la denuncia, el denunciante deberá tener acceso a información fácilmente comprensible sobre todo el proceso. Por ello que la Entidad se compromete a informar debidamente al denunciante de todos los trámites en relación al proceso de denuncia.
b) **Denuncia anónima o nominal**: Decidir si desea formular la comunicación de forma anónima o no anónima; en este segundo caso se garantizará la reserva de identidad del informante, de modo que ésta no sea revelada a terceras personas manteniendo siempre el principio de confidencialidad.
c) **Denuncia verbal o escrita**: Formular la comunicación verbalmente, en persona o por teléfono, o por escrito (mediante el Sistema Interno de Información digital).
d) **Derecho a la utilización de la información con carácter restrictivo**: La información que facilite el denunciante no podrá ser utilizada para fines distintos a los de la investigación.
e) **Derecho a la confidencialidad**: ENSOTRANS MARESME garantiza la confidencialidad en el recibimiento y gestión de las comunicaciones realizadas a través del Sistema Interno de Información. Se informa al denunciante de que, tanto en el formulario de denuncia como durante la investigación, solo se solicitan los datos estrictamente necesarios para tramitarla. Además, solo podrá acceder a dichos datos el personal autorizado.
f) **Acuse de recibo**: Derecho a recibir un "acuse de recibo". La Organización informará al denunciante de la recepción de la comunicación en un plazo máximo de 7 días.
g) **Derecho a recibir una información razonable**: La Organización informará al denunciante del estado de la denuncia en un plazo máximo de tres meses a partir del envío del acuse de recibo.
h) **Derecho a una investigación transparente y a un interlocutor imparcial**: Las denuncias o consultas recibidas serán tratadas con la máxima transparencia e imparcialidad por parte de los encargados de la investigación, que poseen la preparación suficiente y adecuada para responder a las dudas del denunciante o tramitar la denuncia interpuesta.
i) **Derechos derivados de la Protección de Datos**: ENSOTRANS MARESME garantiza que todos los datos que proporcione el denunciante mediante el Sistema Interno de Información serán tratados conforme a la normativa vigente de protección de datos, sin perjuicio de los derechos de los denunciantes.
j) **Derecho a la no represalia**: La Organización recoge la prohibición de represalias al denunciante, por tanto, no se podrá exigir al mismo responsabilidad por la información contenida en la denuncia, salvo que actúe de mala fe.

12.2 Medidas de Protección

Las personas que comuniquen o revelen infracciones previstas en el artículo 2 de la Ley 2/2023, Reguladora de la protección de las personas que informen sobre infracciones normativas y lucha contra la corrupción, tendrán derecho a la protección por parte de ENSOTRANS MARESME, 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 referida Ley 2/2023.
b) La comunicación o revelación se haya realizado conforme a los requerimientos previstos en la referida Ley 2/2023.
c) Que las informaciones que se refieran a acciones u omisiones estén comprendidas en la normativa de referencia. Sin embargo, ENSOTRANS MARESME protegerá todas las denuncias realizadas de buena fe y cuya veracidad sea razonable en los casos de que se denuncie cualquier conducta expuesta en el apartado 5º de la presente Política.
d) Que la denuncia se realice por las personas establecidas en la ley 2/2023 en especial el artículo 3.
e) En el caso de que las informaciones contenidas en comunicaciones que hayan sido inadmitidas por algún canal interno de información según lo dispuesto en la presente Política, las medidas de protección serán aplicables salvo que existan indicios racionales de haberse obtenido dicha información de forma ilícita.
f) Que las informaciones no estén 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.
g) Que las informaciones no estén ya completamente disponibles para el público o que constituyan meros rumores.
h) En caso de personas que hayan comunicado o revelado públicamente información sobre acciones u omisiones de forma anónima pero que posteriormente hayan sido identificadas y cumplan las condiciones previstas en esta Política.
i) Que la comunicación no se realice de mala fe.

12.3 Protección frente a represalias

12.3.1 No se considerará que las personas que comuniquen información sobre las acciones u omisiones recogidas en esta Política y de acuerdo a la normativa aplicable o que hagan una revelación pública de conformidad con esta Política y la normativa aplicable, 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 presente Política y la normativa aplicable.
La referida protección para las personas trabajadoras que informen sobre infracciones del Derecho laboral en materia de seguridad y salud en el trabajo, se entiende sin perjuicio de la establecida en su normativa específica. Esta medida no afectará a las responsabilidades de carácter penal.

12.3.2 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.

12.3.3 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.

12.3.4 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 la presente Política será exigible conforme a la normativa aplicable.

12.3.5 En los procedimientos ante un órgano jurisdiccional u otra autoridad relativos a los perjuicios sufridos por los informantes, una vez que el informante haya demostrado razonablemente que ha comunicado o ha hecho una revelación pública de conformidad con esta Política y que ha sufrido un perjuicio, se presumirá que el perjuicio se produjo como represalia por informar o por hacer una revelación pública. En tales casos, 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.

12.3.6 En los procesos judiciales, incluidos los relativos a difamación, violación de derechos de autor, vulneración de secreto, infracción de las normas de protección de datos, revelación de secretos empresariales, o a solicitudes de indemnización basadas en el derecho laboral o estatutario, las personas a que se refiere el alcance subjetivo de la presente Política no incurrirán en responsabilidad de ningún tipo como consecuencia de comunicaciones o de revelaciones públicas protegidas por la misma.
Dichas personas tendrán derecho a alegar en su descargo y en el marco de los referidos procesos judiciales, el haber comunicado o haber hecho una revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública era necesaria para poner de manifiesto una infracción en virtud de la presente Política.

12.4 Protección del investigado / personas afectadas por la comunicación

La Entidad reconoce los siguientes derechos de la/las Persona/s investigada/s en un expediente en los términos de la presente Política:

a) Establecimiento del derecho del investigado a que se le informe de las acciones u omisiones que se le atribuyen, y a ser oído en cualquier momento. La Entidad se asegurará de que dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.
b) Se reconoce, asimismo, el máximo respeto a la presunción de inocencia, durante la investigación del expediente, el derecho a ser oído, el derecho de defensa, y de acceso al expediente de las personas investigadas.
c) La Entidad reconoce el derecho a la preservación de la identidad de las personas investigadas garantizándose la confidencialidad de los hechos y datos del procedimiento.

d) Durante la tramitación del expediente las personas afectadas por la comunicación tendrán los siguientes derechos:

- Derecho a la presunción de inocencia
- Derecho de defensa
- Derecho de acceso al expediente en los términos regulados en la presente Política y la normativa vigente,
- Igual protección establecida para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

13. PROHIBICIÓN DE REPRESALIAS

13.1 La Entidad prohíbe 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 presente Política y en la normativa aplicable.

13.2 Definición de represalia: 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, sólo por su condición de informantes, o por haber realizado una revelación pública, y siempre que tales actos u omisiones se produzcan mientras dure el procedimiento de investigación o en los dos años siguientes a la finalización del mismo o de la fecha en que tuvo lugar la revelación pública. Se exceptúa el supuesto en que dicha acción u omisión pueda justificarse objetivamente en atención a una finalidad legítima y que los medios para alcanzar dicha finalidad sean necesarios y adecuados.

A los efectos de lo previsto en esta Política y según la ley de aplicación, y a título enunciativo, se consideran represalias las siguientes:

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.

13.3 La persona que viera lesionados sus derechos por causa de su comunicación o revelación una vez transcurrido el plazo de dos años podrá solicitar la protección de la autoridad competente, que, excepcionalmente y de forma justificada, podrá extender el período de protección, previa audiencia de las personas u órganos que pudieran verse afectados. La denegación de la extensión del período de protección deberá estar motivada.

13.4 ENSOTRANS MARESME se compromete a no impedir o dificultar la presentación de comunicaciones y revelaciones, así como a no realizar actos que constituyan represalia o causen discriminación tras la presentación de aquellas al amparo de la ley aplicable, y reconoce que estos actos serán nulos de pleno derecho y darán lugar, en su caso, a medidas correctoras disciplinarias o de responsabilidad, pudiendo incluir la correspondiente indemnización de daños y perjuicios por parte de la Entidad al perjudicado.

13.5 La utilización del Sistema Interno de Información obliga a recordar que la prohibición de represalias prevista en el párrafo anterior no impedirá y puede derivar en responsabilidades penales o civiles y/o medidas disciplinarias que procedan, en los términos contemplados en el ordenamiento vigente y el régimen disciplinario de ENSOTRANS MARESME cuando la investigación interna determine que la comunicación es falsa y que la persona la ha realizado con conocimiento de su falsedad o con temerario desprecio hacia la verdad, decayendo asimismo las exigencias de confidencialidad. De acuerdo con lo establecido en el artículo 456 y siguientes del Código Penal español, la acusación, la denuncia falsa y la simulación de delitos tienen la consideración de delito, sancionable con una pena de prisión de hasta dos años.

14. PROTECCIÓN DE DATOS

14.1 Régimen jurídico del tratamiento de datos personales: los tratamientos de datos personales que deriven de la aplicación de esta Política 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, 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, y en las siguientes disposiciones de este apartado.

No se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una información específica o, si se recopilan por accidente, se eliminarán sin dilación indebida.

14.2 ENSOTRANS MARESME tiene la condición de responsable del tratamiento de los datos personales de conformidad con lo dispuesto en la normativa sobre protección de datos personales.

14.3 El Sistema interno de Información está diseñado, establecido y gestionado de una forma segura, de modo que se garantiza 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.

14.4 El tercero externo que gestione el Sistema Interno de Información tendrá la consideración de encargado del tratamiento a efectos de la legislación sobre protección de datos personales. El tratamiento se regirá por el acto o contrato al que se refiere el artículo 28.3 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

14.5 Respecto a las comunicaciones realizadas verbalmente, se advertirá, en su caso, al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo a lo que establece el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

14.6 Licitud de los tratamientos de datos personales.:

> **14.6.1** se considerarán lícitos los tratamientos de datos personales necesarios para la aplicación de esta Política, 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, así como al art 24 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales:
>
> *Artículo 24 - "Tratamiento de datos para la protección de las personas que informen sobre infracciones normativas: Serán lícitos los tratamientos de datos personales necesarios para garantizar la protección de las personas que informen sobre infracciones normativas. Dichos tratamientos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en esta ley orgánica y en la Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción".*

14.6.2 El tratamiento de datos personales, en los supuestos de comunicación internos, se entenderá lícito en virtud de lo que disponen los artículos 6.1.c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 8 de la Ley Orgánica 3/2018, de 5 de diciembre, y 11 de la Ley Orgánica 7/2021, de 26 de mayo, cuando, de acuerdo a lo establecido en los artículos 10 y 13 de la referida Ley 2/2023 sea obligatorio disponer de un sistema interno de información. Si no fuese obligatorio, el tratamiento se presumirá amparado en el artículo 6.1.e) del citado reglamento.

14.6.3 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.

14.7 Información sobre protección de datos personales y ejercicio de derechos.

14.7.1 Cuando se obtengan directamente de los interesados sus datos personales se les facilitará la siguiente información a que se refieren los artículos 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 11 de la Ley Orgánica 3/2018, de 5 de diciembre. A los informantes y a quienes lleven a cabo una revelación pública se les informa, 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:

1. La identidad y los datos de contacto del responsable y, en su caso, de su representante;
2. Los datos de contacto del delegado de protección de datos, en su caso;
3. Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
4. cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
5. Los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
6. En su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.
7. El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo
8. La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos.
9. Cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.
10. El derecho a presentar una reclamación ante una autoridad de control.
11. Si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos.
12. La existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

14.7.2 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.

14.7.3 Los interesados podrán ejercer los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición a que se refieren los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (artículos 12 y siguientes).

Los afectados tienen 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.

En determinadas circunstancias, podrá solicitar la limitación del tratamiento de sus datos. En tal caso, sólo trataremos 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 cualquier momento y por razones legítimas propias de su situación particular, podrá igualmente oponerse al tratamiento de sus datos. En este caso, dejaremos 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.

Asimismo, y bajo ciertas condiciones, podrá solicitar la portabilidad de sus datos para que sean transmitidos a otro responsable del tratamiento.

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, y presentar una reclamación ante la Autoridad de Control (Agencia Española de Protección de Datos).

Se garantiza el ejercicio de estos derechos por parte del denunciado, sin que ello implique facilitar a aquél datos del denunciante.

Para ejercer sus derechos, en los términos y condiciones previstos en la legislación vigente, deberá remitir una solicitud, acompañada de una copia de su documento nacional de identidad, u otro documento válido que le identifique por correo postal a la dirección: Carrer Remallaire, 15, 08302, Mataró. Barcelona o a la dirección de correo electrónico: ensotrans@ensotrans.com. En el supuesto de que no obtenga una respuesta satisfactoria y desee formular una reclamación u obtener mayor información al respecto de cualquiera de estos derechos, puede acudirse a la Agencia Española de Protección de Datos (www.aepd.es - C/ Jorge Juan, 6 de Madrid).

14.7.4 En caso de que la persona a la que se refieran los hechos relatados en la comunicación o a la que se refiera la revelación pública ejerciese el derecho de oposición, se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales.

14.8. Tratamiento de datos personales en el Sistema interno de información.

14.8.1 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 Organización 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) En su caso, al delegado de protección de datos.

14.8.2 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 Organización o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones a las que se refiere el artículo 2, procediéndose, en su caso, a su

inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación 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.
Si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de los mismos.

14.8.3 Los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.

Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

14.8.4 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 prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

(v) Los empleados y terceros deberán ser informados acerca del tratamiento de datos personales en el marco de los Sistemas de información.

14.9. Preservación de la identidad del informante y de las personas afectadas.

14.9.1 Quien presente una comunicación o lleve a cabo una revelación pública tiene derecho a que su identidad no sea revelada a terceras personas.

14.9.2 Los sistemas internos de información, y quienes reciban revelaciones públicas, no obtendrán datos que permitan la identificación del informante y contarán 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.

14.9.3. La identidad del informante solo 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.

14.9.4 Las revelaciones hechas en virtud de este apartado estarán sujetas a salvaguardas establecidas en la normativa aplicable. En particular, se trasladará al informante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial. Cuando la autoridad competente lo comunique al informante, le remitirá un escrito explicando los motivos de la revelación de los datos confidenciales en cuestión.

15. PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES / COMUNICACIONES (DENUNCIA)

El procedimiento que seguir, tras recibirse una comunicación (denuncia) en los canales internos de comunicación / información de infracciones ("Sistema Interno de Información") será el siguiente. El Responsable del Sistema responderá de la tramitación diligente del procedimiento.

15.1. FASE RECEPCIÓN

15.1.1 Identificación del canal o canales internos de información asociados: las comunicaciones (denuncia) podrán realizarse mediante cualquiera de los canales internos habilitados de comunicación / información de infracciones ("sistema interno de información") establecidos en el apartado 6 de la presente Política.

15.1.2 Además se informa que también podrá realizarse a través de los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

15.1.3 A las comunicaciones (denuncias) recibidas a través de canales internos de información tendrá acceso:

- El miembro de la Organización designado como Responsable del Sistema.
- La persona en quien el Órgano de Gobierno ha delegado las facultades de gestión de los canales internos de comunicación /información ("Sistema interno de Información") y de tramitación de expedientes de investigación.
- En su caso, el tercero externo a quien se haya confiado la gestión de la recepción de informaciones.
- Las personas indicadas en el punto **14.8** de la presente Política.

15.1.4 En caso de recepción de una denuncia, la Presidencia del Comité de Gestión e Investigación de Informaciones convocará a la Secretaría del mismo y deberán reunirse a la mayor brevedad posible y, en todo caso, antes de diez días hábiles desde la recepción de la denuncia (salvo circunstancias excepcionales que lo justificasen).

La asistencia y adopción de acuerdos en las reuniones podrá realizarse, o acudiendo al lugar en que se celebre la reunión o a distancia, por medios electrónicos, incluyendo los telefónicos y audiovisuales, las audioconferencias y las videoconferencias, siempre que todos los miembros dispongan de los medios necesarios, y se reconozca su identidad, y así lo exprese el Acta.

d) Asimismo, siempre que lo decida la Presidencia del Comité de Gestión e Investigación de Informaciones podrán adoptarse por medio del correo electrónico u otro medio similar que permita informar de la denuncia a todos los miembros y conocer la opinión y decisión de todos ellos. Dichas actuaciones deberán quedar reflejadas en el acta de la siguiente reunión, dejando constancia documental, en todo caso, de ellas.

15.1.5 Se establece el deber y garantía de 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. Se establece, asimismo, la obligación del receptor de la comunicación de remitirla inmediatamente al Responsable del Sistema.

En estos supuestos, cuando se tenga conocimiento de la posible infracción a través de los departamentos de la Organización cuya función sea velar por el cumplimiento normativo, así como cuando el conocimiento del hecho llegue por cualquier otra vía, el Comité de Gestión e Investigación de Informaciones procederá del mismo modo referido en el punto anterior.

15.1.6 En el caso de que la denuncia afectase al Compliance Officer o al Responsable del Sistema la persona o personas denunciadas deberá abstenerse de tomar parte en dicha reunión o sistema de adopción de acuerdo.

15.1.7 En el plazo de 7 días naturales siguientes a la recepción de la comunicación (denuncia), y salvo que ello pueda poner en peligro la confidencialidad de la comunicación u otras circunstancias excepcionales que lo justificasen, se procederá a acusar recibo de la misma al informante.

15.2. FASE DE ANÁLISIS Y DE COMUNICACIÓN DE ADMISIÓN / INADMISIÓN A TRÁMITE DE LAS DENUNCIAS.

15.2.1 El Comité de Gestión e Investigación de Informaciones iniciará un análisis preliminar de la información recibida para comprobar si aquella expone hechos o conductas que se encuentran dentro de las conductas denunciables indicadas en la presente Política y si los hechos pudieran ser indiciariamente constitutivos de delito o infracción.

Para realizar el referido análisis preliminar podrá contar con el asesoramiento jurídico o técnico que considere necesario.

Si la denuncia admitida tiene relación con otro expediente ya abierto en el que se investiguen hechos sustancialmente idénticos o conexos, se podrá acordar su acumulación para su tramitación y decisión en un solo procedimiento.

15.2.2 Realizado este análisis preliminar, el Comité de Gestión e Investigación de Informaciones decidirá, en un plazo no superior a quince días hábiles desde la fecha de recepción de la comunicación (denuncia) entre:

15.2.2.1 Inadmitir la comunicación (denuncia) en algunos de los siguientes casos:

a) Cuando los hechos relatados en la comunicación sean manifiestamente infundados o inverosímiles o se evidencie inexistencia de indicios razonables para soportar la misma.

b) Descripción de los hechos de forma genérica, imprecisa o inconcreta. Previo a la inadmisión de una denuncia por esta causa, el Comité de Gestión e Investigación de Informaciones comunicará al denunciante las deficiencias de su denuncia y le otorgará un plazo de 5 días hábiles desde la comunicación al denunciante a fin de que aclare, precise o concrete debidamente los hechos a que se refiera. De no subsanarse tales deficiencias en el citado plazo, se procederá a la inadmisión a trámite de dicha denuncia.

c) Cuando los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico incluida en el ámbito de la ley de aplicación o dentro de las conductas recogidas en el alcance objetivo establecido en la presente Política.

d) Cuando la comunicación carezca manifiestamente de fundamento o existan, a juicio del Comité de Gestión e Investigación de Informaciones, indicios racionales de haberse obtenido dicha información de forma ilícita. En este último caso, siempre que pudiera ser constitutivo de delito, el Comité, previa aprobación del Órgano de Gobierno, podrá remitir a la autoridad judicial competente dicho hecho que se estime constitutivo de delito.

e) Cuando la información sea mera reproducción de otra anterior previamente inadmitida o debidamente investigada.

f) Cuando la comunicación no contenga información nueva y significativa sobre infracciones en comparación con una comunicación anterior respecto de la cual han concluido los correspondientes procedimientos, a menos que se den nuevas circunstancias de hecho o de Derecho que justifiquen un seguimiento distinto

g) Incumplimiento de los requisitos de forma exigidos.

En el supuesto de que por la complejidad de la denuncia el Comité de Gestión e Investigación de Informaciones considera que se requiere de un plazo superior al indicado, podrá establecer un plazo superior que no excederá de 30 días hábiles desde la recepción de la denuncia.

Si concurre alguna o algunas de estas causas se denegará la admisión a trámite de la denuncia, procediéndose a su archivo y no iniciándose por tanto una investigación.

En todo supuesto de inadmisión, el Comité de Gestión e Investigación de Informaciones procederá a informar al informante por escrito y en la dirección de contacto por él facilitada de la decisión de inadmisión, indicando y motivando suficientemente la causa de inadmisión que concurra, en un plazo no superior a treinta días hábiles a partir del acuse de recibo, salvo circunstancia excepcional que justificase un plazo mayor. Ello salvo que la comunicación sea anónima, el informante hubiera renunciado a recibir comunicaciones o no se tenga ninguna forma de comunicación con dicho informante. El expediente quedará cerrado con la notificación. El denunciante podrá incluir la información que considere a efectos de volver abrir el expediente, y la decisión de inadmisión no impedirá una ulterior admisión a trámite e iniciación posterior de una investigación si se recibiera información adicional.

15.2.2.2 Acordar el archivo provisional o definitivo en el supuesto de que los hechos denunciados se hallaran “sub judice”, en espera de que recaiga resolución firme, cuando se decida su comunicación inmediata a la autoridad, entidad u organismo competente para su investigación o cuando se aprecie que la organización no dispone de capacidad /recursos para abordar la investigación.

15.2.2.3 Admitir a trámite la comunicación (denuncia):

Si la comunicación (denuncia) formulada no presenta ninguna de las referidas causa de inadmisión y cumple con los requisitos definidos, el Comité de Gestión e Investigación de Informaciones acordará su admisión a trámite, procederá a informar al informante (denunciante) por escrito y en la dirección de contacto por él facilitada de la decisión de admisión a trámite, en un plazo no superior a 30 días hábiles desde a partir del acuse de recibo, salvo circunstancia excepcional que justificase un plazo mayor, salvo que la comunicación se haya realizado por vía anónima, el informante hubiera renunciado a recibir comunicaciones o no se tenga ninguna forma de comunicación con dicho informante. Se procederá de acuerdo a la política de investigaciones internas de la Organización.

La admisión a trámite se reflejará en el expediente, y se procederá de acuerdo a la política de investigaciones internas de la Organización.

En el caso de que los hechos fueran claramente veraces y pudieran ser indiciariamente constitutivos de delito, el Órgano de Gobierno de ENSOTRANS MARESME remitirá la información al Ministerio Fiscal con carácter inmediato. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

15.2.3 En cualquier caso se establece la posibilidad de mantener la comunicación con el informante y, si se considera necesario, de solicitar a la persona informante información adicional.

15.3 FASE DE INSTRUCCIÓN (INVESTIGACIÓN INTERNA) Y RESOLUCIÓN DEL EXPEDIENTE Y REPORTING.

15.3.1 Se aplicará la "Política de Investigaciones Internas" de la Organización.

15.3.2 En la Política de Investigaciones Internas:

- Se determina el plazo máximo para dar respuesta a las actuaciones de investigación, que será de tres meses a contar desde la recepción de la comunicación (denuncia) 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.

- Se establece 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.

  Si a juicio del Comité de Gestión e Investigación de Informaciones existe riesgo de que la notificación a la persona afectada (denunciada) comprometa o frustre la investigación, o facilite la destrucción o alteración de pruebas, dicha comunicación podrá aplazarse hasta que el citado riesgo desaparezca. En todo caso, el plazo para informar al denunciado no excederá de 1 mes desde la fecha en que se haya acordado la admisión a trámite de la denuncia e iniciar una investigación interna, con la posibilidad de extender dicho plazo a un máximo de 3 meses desde dicha fecha si existen razones justificadas para ello. Todo ello sin perjuicio de que la ley pueda establecer, expresamente y de forma vinculante, unos plazos distintos, en cuyo caso éstos serán los que se deban atender.

- Se exige en todo momento el respeto a la presunción de inocencia y al honor de las personas afectadas.

- Se exige en todo momento respeto de las disposiciones sobre protección de datos personales de acuerdo a lo previsto en la presente Política y normativa vigente de aplicación.

- Se establece la obligación de 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.

15.4. MEDIDAS DE SEGURIDAD.

La Organización se asegurará de que se adopten todas las medidas técnicas y organizativas necesarias para preservar la seguridad de los datos recabados al objeto de protegerlos de divulgaciones o accesos no autorizados, así como el correcto registro de las comunicaciones recibidas.

16. COMUNICACIÓN INTERNA, FORMACIÓN Y SENSIBILIZACIÓN

16.1 Sin perjuicio de la información a proporcionar establecida en el apartado 8 de la presente Política (publicidad del sistema interno de información), a través de la web corporativa de la Organización, se realizará una comunicación de la presente Política a todos los Miembros de la Organización.

16.2 Asimismo se incluirá en las actividades formativas en materia de ética corporativa y cumplimiento normativo que se lleven a cabo para los Miembros de la Organización, con el objetivo de reforzar que estén debidamente informados de los aspectos de la presente Política, y, en especial, cuando haya un cambio relevante en la presente Política o en la normativa reguladora.

16.3 ENSOTRANS MARESME también realizará acciones de comunicación interna y de sensibilización de forma periódica como herramienta de prevención de incumplimientos dentro de la organización.

17. REVISIÓN Y ACTUALIZACIÓN DE LA POLÍTICA Y EL SISTEMA INTERNO DE INFORMACIÓN

17.1 La presente Política y el Sistema Interno de Información será revisado cuando:

- Exista una modificación de la normativa aplicable
- Se necesiten adaptaciones a recomendaciones realizadas por la autoridad competente
- En el caso de que la Entidad quiera hacer mejoras y/o aclaraciones en la Política o Sistema Interno de Información.
- En todo caso, se realizará una revisión anual del contenido de la Política y del buen funcionamiento del Sistema Interno de Información.

17.2 Cualquier revisión y/o actualización deberá ser aprobada por el órgano correspondiente y comunicado de forma efectiva a los Miembros de la Organización siempre que dicha modificación sea sustancial para la compresión de la Política o del funcionamiento del Sistema Interno de Información.

No se publicarán las actualizaciones puramente de formato o de corrección de erratas.

18. DISPOSICIÓN TRANSITORIA

La presente Política resultará de aplicación a todos aquellos hechos cometidos con posterioridad a su entrada en vigor de conformidad a la Disposición Final o que, aun habiéndose cometido con anterioridad a la fecha de su entrada en vigor, se denunciasen con posterioridad a dicha fecha.

19. DISPOSICIÓN FINAL

La presente Política y sus modificaciones serán exigibles a todas las personas a las que resulta de aplicación a partir del momento de su aprobación y comunicación corporativa a través de la página web corporativa.