PROTOCOLO SISTEMA INTERNO INFORMACIÓN Y PROCEDIMIENTO CANAL DE DENUNCIAS

INDICE

I.- INTRODUCCIÓN Y MARCO NORMATIVO

Nuestra organización está firmemente comprometida en fomentar una cultura de cumplimiento normativo como principio de nuestro compromiso ético y de responsabilidad en nuestra empresa y en nuestro entorno. Rechazamos las conductas y actividades irregulares que no solo perjudican a nuestra empresa, clientes y proveedores, sino en general al conjunto de nuestra sociedad.

Con la finalidad de prevenir y evitar dichas conductas, y proteger a quienes informen sobre ellas de forma eficaz, la organización empresarial KAROSSERIEWERKE DRESDEN S.L.U. / KWD ESPAÑA S.L.U. se ha dotado de un Sistema Interno de Información como instrumento orientado al fortalecimiento de la cultura de la información e integridad y de comunicación de la organización, que permita detectar incumplimientos normativos y actos de corrupción conforme a lo dispuesto por la Ley 2/2023 de 20 de febrero.

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, publicada en el BOE número 4, de 21 de febrero, (en adelante la Ley) 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 incorpora los dos objetivos principales de la Directiva, que son el de "*proteger a las personas que informen sobre vulneraciones del ordenamiento jurídico*" y establecer "*los aspectos mínimos que han de satisfacer los distintos cauces de información*".

El presente Procedimiento de KWD ESPAÑA S.L.U junto con la Política del Sistema Interno de Información de la organización, responde a la obligación que establece el artículo 5.2 h), i) y j) de la Ley de contar con una política o estrategia que enuncie los principios generales en materia de sistemas internos de información y defensa de la persona informante, y contar con un procedimiento de gestión de las informaciones recibidas, estableciendo las garantías para la protección de los informantes en el ámbito de la organización.

El sistema interno de la organización se articula en torno a tres elementos:

1.- Canal interno.
2.- Responsable del Sistema de Información.
3.- Procedimiento de gestión de informaciones.

El presente procedimiento se aplicará a las denuncias del resto de empresas del GRUPO SCHNELLECKE LOGISTICS.

II.-CONCEPTO Y OBJETIVO

El Canal de Denuncias se establece no sólo para dar cumplimiento a un requisito legal impuesto por la Directiva 2019/1937 de 23 de octubre, sino para posibilitar que los empleados y terceros puedan comunicar a la organización incumplimientos de normas, ya sean impuestas por el legislador como aquellas que de forma voluntaria se ha dado la propia organización para cumplir con sus principios y fines.

El ámbito de su aplicación alcanza tanto a los empleados (Órgano de gobierno, alta dirección, directivos, mandos intermedios, trabajadores, extrabajadores y otros) como a terceros (clientes, proveedores, consultores externos, etc.), todos los cuales pueden ser denunciantes-informantes.

Por la experiencia obtenida, los denunciantes se sienten más cómodos denunciando por canales internos, es decir, dentro de la organización donde trabajan. Por ello, los objetivos primordiales de la Directiva 2019/1937 son:

- Proteger jurídicamente a aquellas personas que se prestan a denunciar los incumplimientos y que, como consecuencia de ello, pudieran ser represaliadas de muy diversas formas, como por ejemplo el despido, el cambio de puesto de trabajo, la pérdida de contrato en caso de ser un proveedor, etc.
- Fomentar el uso de esta herramienta de comunicación a nivel europeo.

La denuncia podrá ser anónima o nominativa, pero en ambos casos se trata de un procedimiento confidencial por parte de las personas que intervengan en el mismo, estando obligada la Organización a prestarle protección jurídica y evitar cualquier tipo de represalia.

En cuanto a qué debemos entender como infracción, debemos incluir todos aquellos incumplimientos que se produzcan contra la legalidad y contra las normas internas de la Organización, es decir, su Código Ético, las Políticas que lo desarrollan y sus procedimientos. A modo de ejemplo, los casos de corrupción y soborno, conflictos de intereses, fraudes y estafas, medio ambiente, seguridad de los alimentos, manipulaciones contables, acoso y discriminación, violación del Código Ético y otras.

El denunciante será informado en un plazo máximo de tres meses de la tramitación de la denuncia, sus avances o incluso su archivo por falta de pruebas. Dicho plazo podrá ampliarse a seis meses cuando las circunstancias o complejidad del caso lo requiera.

Anualmente se elaborará un informe sobre los procedimientos de denuncias internas que se hayan producido, siendo accesible su conocimiento a empleados y terceros, y poniéndolo en valor en ciclos formativos sobre ética e integridad.

Por otra parte, el presente procedimiento protege igualmente los derechos de la persona afectada por la denuncia (el denunciado), como es la reputación y la confidencialidad de su identidad, así como garantizar sus derechos de defensa, incluido el derecho de acceso al expediente, el derecho a ser oído y el derecho a la tutela judicial efectiva.

III.- AMBITO DE APLICACIÓN DEL SII

a). Ámbito material:

El Sistema interno de información debe permitir la recepción de comunicaciones de información relativas a hechos que pudieran suponer, dentro del ámbito de competencias de LA ORGANIZACIÓN:

A) **Acciones u omisiones** que puedan constituir i**nfracciones del Derecho de la Unión Europea** siempre que:

1.- Entren dentro del ámbito de aplicación de los actos de la Unión enumerados en el Anexo de la Directiva (UE) 2019/1937, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno.

A tal efecto, debe tenerse presente que la citada Directiva establece normas mínimas comunes para la protección de las personas que informen sobre las siguientes infracciones del Derecho de la Unión:

a) infracciones que entren dentro del ámbito de aplicación de los actos de la Unión enumerados en el anexo relativas a los ámbitos siguientes:

i) contratación pública, ii) servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo, iii) seguridad de los productos y conformidad, iv) seguridad del transporte, v) protección del medio ambiente, vi) protección frente a las radiaciones y seguridad nuclear, vii) seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales, viii) salud pública, ix) protección de los consumidores, x) protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información.

2.- 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

3.- Incidan en el mercado interior, tal y como se contemplan en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión 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 a prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades.

B) **Acciones u omisiones** que puedan ser constitutivas de **infracción penal o administrativa grave o muy grave** y estén relacionadas con las siguientes materias:

a. Contratación pública
b. Servicios, productos y mercados financieros, prevención de blanqueo de capitales y financiación del terrorismo
c. Seguridad de los productos y conformidad
d. Seguridad del transporte
e. Protección del medio ambiente
f. Protección frente a las radiaciones y seguridad nuclear
g. Seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales

h. Salud pública

i. Protección de los consumidores y usuarios

j. Protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información

k. Conductas de acoso, acoso sexual y acoso por razón de sexo

En todo caso, se entenderán comprendidas todas aquellas infracciones penales o administrativas graves o muy graves que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.

C) **Infracciones del derecho laboral** en materia de seguridad y salud en el trabajo de las que informen los trabajadores, sin perjuicio de lo establecido en su normativa específica.

D) **Actuaciones contrarias** a las Políticas corporativas de nuestro Sistema de Compliance

Se incluyen en el ANEXO II las actividades ilícitas que se pueden aplicar a nuestra organización.

b) **Ámbito personal: personas informantes**

Serán objeto de recepción, tramitación y seguimiento las informaciones recibidas de las personas informantes que trabajen en el sector privado o público y que hayan obtenido información sobre infracciones en el contexto laboral o profesional de nuestra organización comprendiendo en todo caso:

- Las personas que tengan la condición de rabajadores o trabajadoras por cuenta ajena.
- Las personas autónomas.
- Las personas accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de nuestra organización, incluidos los miembros no ejecutivos, así como los voluntarios y trabajadores en práctica, remunerados o no.
- Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.
- Las personas informantes que comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral o estatutaria ya finalizada
- Aquellas personas informantes cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.

IV.- DEFINICIONES

i. **Infracciones:** las acciones u omisiones que sean ilícitas y estén relacionadas con las siguientes materias:
    a. Contratación pública
    b. Servicios, productos y mercados financieros, prevención de blanqueo de capitales y financiación del terrorismo
    c. Seguridad de los productos y conformidad
    d. Seguridad del transporte
    e. Protección del medio ambiente
    f. Protección frente a las radiaciones y seguridad nuclear
    g. Seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales
    h. Salud pública
    i. Protección de los consumidores y usuarios
    j. Protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información
    k. Conductas de acoso, acoso sexual y acoso por razón de sexo

i. **Información sobre infracciones**: la información, incluidas las sospechas razonables, sobre infracciones reales o potenciales que se hayan producido o se vayan a producir en la organización en la que trabaje o haya trabajado el denunciante o en otra organización que, por motivo de trabajo, haya estado en contacto el denunciante; y sobre intentos de ocultar tales infracciones
ii. **Denuncia/Información o denunciar**: la comunicación verbal o por escrito de información sobre infracciones
iii. **Denuncia/Información interna**: la comunicación verbal o por escrito de información sobre infracciones dentro de una entidad jurídica de los sectores privados o públicos.
iv. **Denuncia/Información externa**: la comunicación verbal o por escrito de información sobre infracciones ante las autoridades competentes.
v. **Revelación pública o revelar públicamente**: la puesta a disposición del público información sobre infracciones.
vi. **Denunciante/Informante**: persona física que comunica o revela públicamente información sobre infracciones obtenida en el contexto de sus actividades laborales.
vii. **Facilitador/a**: persona física que asiste a un denunciante en el proceso de denuncia en un contexto laboral y cuya asistencia debe ser confidencial.
viii. **Contexto laboral**: las actividades de trabajo presentes o pasadas en el sector público o privado a través de las cuales, las personas pueden obtener información sobre infracciones y en el que estas personas podrían sufrir represalias si comunicaran dicha información.
ix. **Persona afectada**: persona física o jurídica a la que se haga referencia en la denuncia/información o revelación pública como la persona a la que se atribuye la infracción o con la que se asocia la infracción
x. **Represalia**: toda acción u omisión, directa o indirecta, que tenga lugar en un contexto laboral, que esté motivada por una denuncia o revelación pública y que cause o pueda causar perjuicios injustificados al denunciante.

xi. **Seguimiento**: toda acción emprendida por el destinatario de una denuncia o autoridad competente a fin de valorar la exactitud de las alegaciones hechas en la denuncia y, en su caso, resolver la infracción denunciada, incluso a través de investigaciones internas, acciones judiciales, acciones de recuperación de fondos o el archivo del procedimiento.

xii. **Respuesta**: la información facilitada a los denunciantes sobre las medidas previstas o adoptadas para seguir la denuncia y los motivos de tal seguimiento

xiii. **Autoridad competente**: toda autoridad nacional designada para recibir denuncias y dar respuesta a los denunciantes, y hacer el seguimiento.

V.- RESPONSABLE DEL SISTEMA INTERNO INFORMACION - GESTION DEL CANAL

a) Nombramiento y Registro:

El Responsable del Canal de Denuncias es nombrado, destituido y cesado por el de órgano de administración, en nuestra organización el Consejo de Administración de KWD ESPAÑA S.L.U., de entre los miembros de la alta dirección de la organización.

El Consejo de Administración de la organización KWD ESPAÑA S.L.U. ha procedido al nombramiento del Responsable del Sistema Interno de Información a una persona integrante de la misma con cargo en la alta dirección, el Director del Departamento de RRHH, quien ha aceptado la designación, ha prometido ejercerlo leal y fielmente, y afirmado no afectarle ninguna incompatibilidad para el ejercicio del cargo.

En el caso de existir conflicto de intereses que afectare a la Dirección de RRHH, las personas designadas para la instrucción del expediente serán las que integren la Comisión de Gerencia.

El Responsable podrá contar con asesores consultivos o que puedan colaborar en determinadas ocasiones.

El nombramiento, destitución y cese del Responsable del Canal de Denuncias, será comunicado a la Autoridad Independiente de Protección del Informante (A.A.I) en el plazo de los 10 días hábiles siguientes, especificando, en el caso de su cese, las razones que han justificado el mismo.

b) Funciones:

En cumplimiento de la Directiva (UE) 2019/1937 y a las respectivas leyes aprobadas en el ordenamiento jurídico propio de cada Estado, y sin que sean limitativas, la organización KWD ESPAÑA S.L.U. asigna al Responsable del Sistema Interno de Información las siguientes funciones:

a) Diseño del Sistema Interno de Información aprobado
b) Elaboración, desarrollo de las políticas y procedimientos
c) Verificación y tramitación diligente de la aprobación por el órgano de gobierno del procedimiento de gestión de las informaciones.

d) Tramitación de su nombramiento /revocación ante la Autoridad Independiente de Protección del Informante-AAI
e) Implantación y Gestión del Sistema Interno de Información
f) Supervisión del funcionamiento y cumplimiento del Sistema Interno de Información
g) Formación/información sobre el Sistema Interno de Información
h) Gestión del CANAL DE DENUNCIAS
i) Gestión de las acciones de Comunicación.
j) Gestión del Libro-Registro de informaciones
k) Tramitación de los expedientes derivados del Canal de Denuncias
l) Verificación y seguimiento medidas para la protección de las personas informantes
m) Elaboración de una memoria anual.
n) Revisión y actualización del SII, cuando sea el caso.

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

El Consejo de Administración velará por garantizar que la persona designada para asumir ese cargo solo desempeñe otras funciones cuando estas sean compatibles con el cargo de Responsable del Canal de Denuncias y siempre que no supongan un conflicto de interés para el desempeño del puesto de Responsable del Canal de Denuncias.

c) Personas y entidades implicadas en la gestión del canal:

El gestor directo del canal es ser un gestor externo a la organización (GFM SERVICIOS), contratado al efecto, que se encargará de proporcionar y mantener el canal de denuncias, garantizando la confidencialidad de las comunicaciones realizadas. Asimismo, se encargará de analizar preliminarmente el contenido de los hechos que son objeto de información y de asesorar al Responsable del Sistema interno de Información en la gestión del Canal de denuncias y en la implantación del propio Sistema interno de Información.

No obstante, será el órgano de administración o el órgano de gestión de la organización quien designe a la persona física que será el Responsable interno del canal de denuncias y recibirá las denuncias e informes elaborados por el Gestor, tramitando cada denuncia de conformidad con las recomendaciones indicadas por éste y en atención a la gravedad y contenido de las denuncias. El Responsable del Canal de Denuncias reportará y colaborará en todo momento con el Responsable de Cumplimiento Normativo (Compliance Officer) en su caso.

Solo participarán en la gestión y tramitación de las denuncias el Responsable del Canal de Denuncias, el Responsable de Cumplimiento Normativo y el gestor externo.

VI.- CANALES DE DENUNCIA

a) Nuestro Sistema Interno de Información se encuentra integrado por los siguientes **canales internos:**

- Canal interno de comunicación de infracciones.
- Canal de denuncias del Sistema de Compliance con dominio kwdag o el que corresponda a la empresa en cada momento.
- Canal interno de denuncias de acoso sexual y acoso por razón de sexo previsto en el protocolo de prevención aprobado en el Plan de Igualdad.

b) **Canales externos**

Además de utilizar el canal interno de nuestra organización que se desarrolla en este documento, toda persona física que lo desee puede presentar su información a través del canal externo de información de la Autoridad Independiente de Protección del Informante (A.A.I.).

Además, cualquier persona que tenga conocimiento de hechos que pudieran ser constitutivos de fraude o irregularidad podrá ponerlos en conocimiento a través de las direcciones webs de los organismos nacionales e internacionales que se relacionan en el Anexo I de este Procedimiento.

VII.- PROCEDIMIENTO

Con la finalidad de asegurar que el sistema sea gestionado de forma segura, la organización KWD ESPAÑA S.L.U. cuenta con los servicios del aplicativo informático para la remisión de comunicaciones.

Esta herramienta permite la presentación de informaciones objeto de protección por el presente procedimiento de forma segura, en aplicación tanto de la normativa nacional como la Directiva 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.

El Responsable del Sistema interno de Información de la organización será la figura encargada de supervisar que las soluciones técnicas utilizadas para el soporte de los canales internos se adecúan a los requisitos mínimos de seguridad y confidencialidad establecidos por la normativa de aplicación y por el presente procedimiento.

El sistema tecnológico adoptado cuenta con medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos de las personas afectadas y cualquier tercero que se mencione en la comunicación. Asimismo, el sistema cuenta con garantías de cumplimiento de protección de la normativa RGPD. Las comunicaciones efectuadas por el canal se encuentran cifradas de extremo a extremo y cuenta con garantías de que no se podrán trazar las direcciones de IP.

A través de la plataforma implantada se podrán presentar comunicaciones de forma escrita, verbal o de ambos modos, garantizándose la confidencialidad del informante e incluso la garantía de presentar comunicaciones de forma anónima.

Todos los canales de comunicación integrados en el sistema de información de nuestra organización se encuentran integrados en la solución informática utilizada por la organización, como CANAL UNICO DE DENUNCIAS.

FASES:

a) Formalización información, recepción y registro

La persona que conozca la existencia de una situación o conducta irregular, incumplimiento o vulneración deberá reportarla inmediatamente.

El Canal de Denuncias constituye el principal medio a través del cual se efectuarán las comunicaciones e informaciones.

La comunicación a través del Canal de Denuncias podrá realizarse accediendo a la plataforma con acceso desde nuestra web.

En caso de que la comunicación que se reciba no sea anónima, se reservará en todo caso la identidad del informante y se adoptarán las medidas necesarias para garantizar la confidencialidad y de la información objeto de la comunicación y los derechos del informante.

Igualmente, se podrá solicitar una reunión presencial con el gestor del Canal de Denuncias a la que acudirán dos personas de ese equipo y que tendrá lugar en el plazo máximo de siete días desde la solicitud efectuada por el informante.

Cuando la comunicación se realice de manera verbal, se advertirá al informante de que ésta será grabada o transcrita y se le informará del tratamiento de sus datos de conformidad con la normativa de aplicación. Sin perjuicio de los derechos que le corresponden de acuerdo con la normativa de protección de datos, se ofrecerá al informante la oportunidad de revisar la transcripción para comprobar, rectificar y aceptar mediante su firma el contenido.

Las comunicaciones realizadas a través de este Canal deberán recoger la siguiente información a fin de facilitar la asignación para su tramitación, investigación y gestión:

- Identificación del informante cuando se opte por realizar la comunicación de forma confidencial y no anónima. A tal efecto, se deberá indicar el nombre y apellidos y una dirección de contacto.
- Identificación de la persona a la que se refieren los hechos sobre los que se informa, en su caso.
- Descripción básica de los hechos comunicados, indicando (si fuera posible) las fechas en las que han tenido lugar; y
- Elementos sobre los que se basa la sospecha de la comisión de irregularidades.

Una vez recibida la comunicación, independientemente del medio utilizado, se procederá a su registro, se le asignará un código de identificación y quedará registrada de forma segura y con acceso restringido a las personas autorizadas para ello, y remitirá un acuse de recibo al informante en un plazo máximo de 7 días naturales.

b) Evaluación preliminar para admisión

El Responsable del SII junto con el gestor del Canal de denuncias, será quien reciba las comunicaciones y realicen una evaluación preliminar de las mismas con el fin de verificar que se encuentran dentro del ámbito de aplicación del Canal de Denuncias.

En caso de reunir los requisitos mínimos, se admitirá la información recibida y se procederá a la apertura de la investigación interna para esclarecer los hechos sobre los que se ha informado y comprobar su veracidad.

En los casos en que se requiera información adicional del denunciante para iniciar o continuar con la investigación, la información será solicitada y deberá recibirse en 15 días o el caso será cerrado y clasificado como "información insuficiente".

Por el contrario, para los supuestos en los que se considere por parte del Responsable del Sistema de Información (o de las personas que integran la Comisión de Gerencia en supuesto de conflicto de intereses) de que la comunicación incurre en cualquiera de las causas tasadas de inadmisión, se deberá comunicar dicha circunstancia por escrito al informante dentro del plazo establecido más adelante, especificando la causa por la que se ha inadmitido la investigación de los hechos comunicados.

Una vez realizado el análisis preliminar se decidirá por el Responsable de la gestión del Canal, en un plazo que no podrá ser superior a diez días hábiles desde la fecha de entrada al Canal de Denuncias de la comunicación, (prorrogándose el plazo en el caso de solicitar más información) si se admite a trámite o no, informando, en su caso, de la decisión, salvo que la comunicación sea anónima o el informante hubiera renunciado a recibir comunicaciones sobre la denuncia realizada.

No se admitirán a trámite a través del Canal de Denuncias aquellas comunicaciones que se refieran a:

- Hechos que carezcan de total verosimilitud;
- Hechos que no se refieran a alguna de las materias objeto de este Procedimiento o solo contengan meras opiniones personales o valoraciones subjetivas ajenas a la finalidad de este Canal;
- Comunicaciones que carezcan manifiestamente de fundamento;
- Comunicaciones que no aporten información nueva sobre otras anteriores;
- Comunicaciones que pongan de manifiesto indicios racionales de haberse obtenido la información mediante la comisión de un delito. En este caso, además de la inadmisión, se remitirá la comunicación a la Dirección Legal para que proceda a la comunicación al Ministerio Fiscal de una relación circunstanciada de los hechos que se estimen constitutivos de delito.

En estos casos, se archivará la comunicación dejando constancia razonada de esta decisión en el registro del Canal de Denuncias.

La decisión de archivo no impedirá la iniciación posterior de una investigación si se recibiera información adicional de acuerdo con lo establecido en la Política del Canal de Denuncias.

c) Procedimiento/gestión de la información y notificaciones

En caso de admitir a trámite la comunicación, los gestores del Canal la remitirán al Responsable para que a su vez las comunique a las personas o Comisiones, en su caso, con funciones encargadas de la investigación, que serán las siguientes:

- Cuando la comunicación se refiera a incumplimientos de obligaciones legales relativas a principios éticos relacionados con respeto a las personas, discriminación, igualdad de trato y oportunidades, conciliación del trabajo y vida personal, prevención de riesgos laborales o derechos colectivos, se remitirá a la Dirección de RRHH, que será quien se encargue de llevar a cabo la investigación y proponer la resolución de la comunicación y adopción de medidas que la Dirección considere adecuadas.

- Cuando la comunicación se refiera a conductas que puedan ser constitutivas de acoso sexual o acoso por razón de sexo, se remitirán a la Comisión de Igualdad para la activación del protocolo de prevención del acoso sexual y acoso por razón de sexo, aperturando en su caso la Comisión Instructora el oportuno expediente. A fin de velar por el procedimiento del canal de denuncias la Comisión Instructora deberá facilitar de manera confidencial y anonimizada los datos del expediente necesarios para el registro de la denuncia en el Canal de Denuncias.

- Las comunicaciones en las que se refieran conductas contrarias a los comportamientos corporativos de la organización se remitirán al Compliance Officer a fin de que intervenga junto al RSII en la investigación, gestión y resolución de estos casos.

- Las comunicaciones relativas a Blanqueo de Capitales y Financiación del Terrorismo (BC/FT), se remitirán al Compliance Officer, o en su defecto al Responsable de Prevención del Blanqueo de Capitales que será quien intervenga junto al RSII a fin de tramitar, investigar, en su caso, emitir resolución para proponer a la Dirección adoptar las medidas precisas de acuerdo con la legislación vigente y normativa interna en dicha materia.

- Las comunicaciones que se reciban y refieran materias que no estén contempladas en los puntos anteriores, serán gestionadas por el Responsable del SII

En aquellos casos en los que por su complejidad o gravedad se considere necesario se podrá constituir un equipo de investigación formado por el Responsable del SII, con el Compliance Officer y el Responsable de RRHH (si fuera persona diferente al RSII), que contarán con categoría y autonomía suficiente para llevar a cabo la investigación y participar en la toma de decisiones que se requieran.

A la vista de la especificidad del caso que se trate, se podrá solicitar la colaboración de un asesor externo. para lo cual será necesario contar con un contrato de prestación de servicios, contar con un contrato de encargado de tratamiento y establecer un acuerdo de confidencialidad.

d) Apertura, investigación y resolución expediente

La investigación comprenderá todas aquellas actuaciones encaminadas a comprobar la veracidad de los hechos relatados en la comunicación recibida y si son constitutivos de alguno de los incumplimientos objeto de este Procedimiento.

a) Entrevista a la persona afectada por la información

Siempre que sea posible, se llevará a cabo una entrevista con la persona afectada por la información en la que se le invitará a exponer su versión de los hechos y a aportar los medios de prueba que considere adecuados y pertinentes.

En esta entrevista se informará a la persona investigada de los hechos que se le atribuyen de manera sucinta, sin revelar la identidad del informante ni dar acceso a la comunicación, a fin de que pueda alegar lo que considere oportuno para defenderse, de acuerdo con las garantías de este Procedimiento, especialmente:

- Derecho a la presunción de inocencia, a ser oída, a la defensa y a presentar alegaciones.
- Derecho a la protección contemplada para los informantes en la Ley 2/2023.
- Información de la política de privacidad y de tratamiento de datos de carácter personal conforme al art.13 RGPD y el ejercicio de los derechos de los arts.15-22 RGPD, aunque se le advertirá que, en caso de ejercer el derecho de oposición, se presumirá la existencia de motivos legítimos que legitiman el tratamiento de sus datos personales.

Las entrevistas se documentarán por escrito en un acta indicando los asistentes, asuntos tratados y conclusiones, que firmarán tanto persona afectada por la información, como las personas que le entrevisten.

b) Acceso a dispositivos electrónicos

Cuando resulte necesario el acceso a los dispositivos electrónicos de los empleados, se realizará, previa autorización del Director de Recursos Humanos y del Compliance Officer, en su caso.

El acceso a la información contenida en los dispositivos electrónicos de los empleados, titularidad de la organización, se hará garantizando el derecho a la intimidad del empleado, recabando únicamente aquella información que sea estrictamente necesaria y pertinente para el buen fin de la investigación.

El acceso a los dispositivos electrónicos se llevará a cabo, en todo caso, de acuerdo con la Política interna sobre las normas de usos de dispositivos.

c) Investigación e Informe

Las investigaciones internas deberán estar finalizadas en el plazo de 3 meses, que podrá prorrogarse únicamente por causa justificada en los casos de especial complejidad otros 3 meses adicionales, informando de ello al Responsable de la gestión del Canal De Denuncias.

Concluida la investigación, las personas o Comisiones responsables de la instrucción del expediente, resolverán el expediente recogiendo en un informe el resultado alcanzado e indicando en todo caso:

- El código de identificación y fecha de registro
- Una exposición de los hechos relatados en la comunicación
- Medidas cautelares adoptadas, en su caso
- Las actuaciones realizadas con el fin de comprobar la veracidad de tales hechos
- Las conclusiones alcanzadas en la investigación

En todo caso el informe se centrará en los hechos recabados durante la investigación, evitándose expresiones o conclusiones basadas en opiniones personales.

d) Resolución

En base a las conclusiones alcanzadas, el Responsable del Sistema de Información adoptará cualquiera de las siguientes resoluciones:

- Una propuesta de decisión de archivo de la información sin adoptar medidas por falta de fundamentación de la misma o por no verificarse la responsabilidad del investigado; lo que será notificado al informante y, en su caso, a la persona afectada.

  En este supuesto, el informante tendrá derecho a la protección prevista en la Política del Canal De Denuncias y en este Procedimiento.

- La propuesta de decisión de archivar el procedimiento por ausencia de elementos de prueba suficientes para concluir que los hechos comunicados constituyen infracción normativa.

- La conclusión de que los hechos comunicados constituyen infracción normativa: El Responsable del Sistema podrá realizar a la Dirección una propuesta de aplicación de las medidas disciplinarias o acciones judiciales que considere adecuadas, así como de las medidas correctoras en subsanación de las deficiencias o lagunas detectadas en el Sistema Interno de Información.

En los supuestos en los que de la información comunicada pudiesen desprenderse hechos indiciariamente constitutivos de delito, el Responsable (o la Comisión en su caso) del Sistema deberá comunicar dicha situación a la Dirección de la organización y al órgano de administración, a efectos de que determine si se cumplen los requisitos de lo dispuesto por el artículo 9 j) de la Ley 2/2023 de 20 de febrero, para el caso de que se considere que se hubiera podido cometer un delito. En este caso, la Dirección dará instrucciones respecto al modo de proceder para remitir la información al Ministerio Fiscal, o a la Fiscalía Europea en los supuestos que afecten a intereses financieros de la UE; o, en su caso, propuesta de traslado de los resultados de la investigación a las autoridades competentes (administrativas, policiales o judiciales).

e) Conflicto de intereses:

La presentación de una información que afecte directamente a personas que puedan participar activamente en la gestión de esta supondrá su exclusión automática de la gestión de la denuncia. De esta forma, no podrá participar ni en la investigación ni en la decisión final de la investigación ni en la adopción de la sanción quien sea el sujeto afectado por la información.

Si la denuncia afectare directamente al Responsable del Sistema Interno, será la Comisión de Gerencia quien intervenga en la instrucción del expediente y gestión de la denuncia en su sustitución.

f) Denuncias Falsas:

Se considerará toda acusación falsa o maliciosa realizada de manera deliberada por uno de sus empleados como una infracción grave que podrá ser sancionada de conformidad con lo establecido en el régimen de infracciones y sanciones, de acuerdo con la normativa laboral y/o penal.

Conforme establece el Código Penal Español, podríamos estar ante un delito de acusación o denuncia falsa (art. 456 CP) o bien de un delito de calumnias (art. 205 CP).

El Código Penal, en su artículo 456.1, relativo al delito de acusación o denuncia falsa, establece que la persona que, con conocimiento de su falsedad o temerario desprecio hacia la verdad, impute a alguna otra persona hechos que, de ser ciertos, constituirían infracción penal, si esta imputación se hiciera ante funcionario judicial o administrativo que tenga el deber de proceder a su averiguación, será sancionada con la pena de prisión de seis meses a dos años y multa de doce a veinticuatro meses, si se imputara un delito grave; con la pena de multa de doce a veinticuatro meses, si se imputara un delito menos grave; y con la pena de multa de tres a seis meses, si se imputara un delito leve.

El delito de calumnias contemplado en el art. 205 del Código Penal establece que será “calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad” y podrá ser castigada con las penas de prisión de seis meses a dos años o multa de doce a 24 meses, si se propagaran con publicidad y, en otro caso, con multa de seis a 12 meses.

Y en el ámbito de aplicación de la normativa laboral, el art. 58 del Estatuto de los Trabajadores establece que “los trabajadores podrán ser sancionados por la dirección de las entidades en virtud de incumplimientos laborales, de acuerdo con la graduación de faltas y sanciones que se establezcan en las disposiciones legales o en el convenio colectivo que sea aplicable.”

En nuestra organización se aplicará se aplicará el régimen disciplinario establecido en la legislación laboral vigente.

g) Régimen disciplinario:

El incumplimiento del Código Ético o de cualquiera de los manuales o códigos descritos en la presente instrucción, así como cualquier acto supuestamente ilícito o delictivo podrá derivar en medidas disciplinarias, sin perjuicio de las sanciones administrativas o penales que puedan resultar, según proceda, de dichos casos de acuerdo con la legislación laboral aplicable.

Las sanciones dependerán de la gravedad del delito y demás circunstancias.

El Responsable trasladará a Dirección, o en su caso el Comité de Compliance, quién es el órgano competente para evaluar si se ha producido una irregularidad o infracción de cualquier código interno, así como para decidir acerca de las sanciones que se impondrán y encargar a RRHH la puesta en marcha del procedimiento disciplinario contra el o los empleados en relación con los casos de incumplimiento del Código Ético y sus reglamentos de transposición.

Además, si se determina que la conducta de un empleado puede constituir un delito imputable a la organización, se informará al Comité de Cumplimiento y a las autoridades públicas competentes de las medidas legales que se adoptarán. Esta notificación deberá estar justificada por las pruebas y/o indicios que puedan haberse recopilado.

Bajo ninguna circunstancia podrá justificarse un delito por el hecho de que la organización se beneficiaría de ello. La organización rechaza cualquier ingreso o beneficio que pueda derivarse de la conducta de sus empleados o de terceros en contra del Código Ético, Políticas corporativas o Instrucción de Prevención y Detección de delitos.

VIII.- TRATAMIENTO DE DATOS PERSONALES

a) Cumplimiento normativa de protección de datos:

Los tratamientos de datos personales que se deriven de la aplicación de la Ley 2/2023 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.

Los datos de carácter personal facilitados por el informante y los obtenidos de los procedimientos de investigación interna, serán tratados por nuestra organización y por los corresponsables del tratamiento que con nosotros tengan relación, para ser incorporados al Sistema interno de información de protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción atendiendo a los criterios y directrices marcados por la Ley 2/2023, el Reglamento General de Protección de Datos, la Ley Orgánica de Protección de Datos y Garantías de Derechos Digitales.

La finalidad del tratamiento es la protección a las personas que, en un contexto laboral o profesional, detecten posibles infracciones y las comuniquen mediante los mecanismos regulados en la citada norma legal y se tratarán con la exclusiva finalidad de gestionar y tramitar las comunicaciones recibidas, investigar los hechos comunicados, y las eventuales obligaciones legales derivadas

El sistema interno de información impedirá el acceso no autorizado y preservará la identidad y garantizará la confidencialidad de los datos correspondientes a las personas afectadas (persona informante y persona denunciada, en su caso) y a cualquier tercero que se mencione en la información suministrada especialmente la identidad de la persona informante en caso de que se hubiera identificado.

Por ello, la identidad del informante será en todo caso reservada, y no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros. 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. Las revelaciones hechas en virtud de este apartado estarán sujetas a salvaguardas establecidas en la normativa aplicable. En estos casos, con carácter previo a revelar su identidad, se remitirá al informante un escrito explicando los motivos de la revelación, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial.

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.

El derecho de acceso de la persona de la que se refieren las informaciones, se limita a los datos de carácter personal que le conciernan. No se aplica a las otras informaciones contenidas en la información.

La persona a la que se refiera la información podrá pedir la rectificación o la supresión de sus datos personales cuando éstos sean inexactos, incompletos, equivocados, o caducados. Si se establece que la persona ha sido investigada erróneamente, tendrá derecho a hacer suprimir las informaciones que le conciernen.

b) Conservación denuncias

Los datos personales obtenidos de las informaciones recibidas y aquellos que tengan su origen en 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

con la finalidad para la que fueron recabados. En particular, se tendrá en cuenta lo previsto en los apartados 3 y 4 del artículo 32 de la Ley 2/2023, de 20 de febrero:

.- Los datos objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la pro9cedencia de iniciar una investigación sobre los hechos informados

.- En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubieran 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.

.- En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de los hechos objeto de protección por el presente procedimiento, debiendo darse cumplimiento a lo establecido por el Título VI de la Ley 2/2023 de 20 de febrero. Si la información recibida contuviera datos 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.

IX.- MEDIDAS DE PROTECCIÓN

De acuerdo con el Título VII “Medidas de protección” de la Ley 2/2023, de 20 de febrero, el Sistema de información garantizará que las personas que informen sobre infracciones normativas y de lucha contra la corrupción gocen de las siguientes medidas de protección:

a) Personas incluidas en el ámbito de protección:

- Personal vinculado nuestra organización por una relación laboral/ societaria: empleados (o personas trabajadoras o personas que tengan la condición de empleados), socios, personas pertenecientes a los órganos de administración y gestión de nuestra organización, incluidos los miembros no ejecutivos; voluntarios, becarios, trabajadores en período de formación y ex empleados y otras personas anteriormente vinculadas por una relación ya finalizada, respectos a hechos acaecidos durante la relación laboral finalizada ; y aquellas cuya relación no haya comenzado y obtengan información durante el proceso de selección o negociación precontractual.

- Personas con vinculación societaria

- Autónomos, contratistas y subcontratistas la organización, y las personas que trabajen para o bajo la supervisión y dirección de contratistas, subcontratistas y proveedores.

Asimismo, serán de aplicación las medidas de protección frente a represalias previstas en el Sistema Interno de Información a los siguientes:

- Representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante.
- Personas físicas de la organización que asistan al informante en el proceso.
- Personas físicas que estén relacionadas con el informante y que puedan sufrir represalias (compañeros de trabajo, familiares)
- Personas jurídicas para las que trabaje o mantenga una relación de contexto laboral o en las que ostente participación

b) Condiciones de protección

1. Las personas que comuniquen o revelen infracciones de las previstas en el ámbito de este Procedimiento, tendrán derecho a protección siempre que concurran las circunstancias siguientes:
    a) Tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación o revelación, aun cuando no aporten pruebas concluyentes, y que la citada información entra dentro del ámbito de aplicación de la Ley.
    b) La comunicación o revelación se haya realizado conforme a los requerimientos previstos en la Ley.
2. Quedan expresamente excluidos de la protección prevista en la Ley aquellas personas que comuniquen o revelen:
    a) Informaciones contenidas en comunicaciones que hayan sido inadmitidas por algún canal interno de información o por la Autoridad Independiente.
    b) Informaciones vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación o revelación.
    c) Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores.
    d) Informaciones que se refieran a acciones u omisiones no comprendidas en el ámbito de aplicación material de la Ley.
3. Las 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 la Ley, tendrán derecho a la protección que la misma contiene.

Las personas que informen ante las instituciones, órganos u organismos pertinentes de la Unión Europea infracciones que entren en el ámbito de aplicación de la Directiva

(UE) 2019/1937 del Parlamento Europeo tendrán derecho a protección con arreglo a lo dispuesto en la Ley en las mismas condiciones que una persona que haya informado por canales externos.

c) Prohibición de represalias

Dando cumplimiento al artículo 36 de la Ley, nuestra organización se compromete a la no aplicación de ningún tipo de represalia vinculada con su ámbito de aplicación.

Para ello:

1. Se prohíben expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación conforme a lo previsto en la Ley.
2. Se entiende por represalia cualesquier acto u omisión que esté prohibido por la Ley, o que, de forma directa o indirecta, suponga un trato desfavorable que sitúe a las personas que la sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, solo por su condición de informantes, o por haber realizado una revelación pública.
3. A los efectos de lo previsto en la Ley, y a título enunciativo, se consideran represalias las que se adopten en forma de:
    a. Suspensión del contrato de trabajo, despido o extinción de la relación laboral o estatutaria, incluyendo la no renovación o la terminación anticipada de un contrato de trabajo temporal una vez superado el período de prueba, o terminación anticipada o anulación de contratos de bienes o servicios, imposición de cualquier medida disciplinaria, degradación o denegación de ascensos y cualquier otra modificación sustancial de las condiciones de trabajo y la no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido; salvo que estas medidas se llevaran a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral o reguladora del estatuto del empleado público correspondiente, por circunstancias, hechos o infracciones acreditadas, y ajenas a la presentación de la comunicación.

    b. 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.

4. 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 Independiente de Protección del Informante que, excepcionalmente y de forma justificada, podrá extender el período de protección, previa audiencia de las personas u órganos que pudieran verse afectados.

5. Los actos administrativos que tengan por objeto impedir o dificultar la presentación de comunicaciones y revelaciones, así como los que constituyan represalia o causen discriminación tras la presentación de aquellas al amparo de la Ley, 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 al perjudicado.

X.- REGISTRO Y ARCHIVO

El registro de denuncias consistirá en un fichero (gestionado en el aplicativo del Canal) en el que se incluirán las denuncias recibidas, sean admitidas o inadmitidas, a efectos de conservación para dejar evidencia del funcionamiento del Sistema interno de Información, y en especial del CANAL DE DENUNCIAS.

En el caso de las denuncias admitidas, se recogerán todos los datos de los que se dispongan, así como la fecha y hora de introducción de datos en el registro de denuncias, fecha y hora de recepción de la denuncia en el buzón del canal de denuncias y fecha de la decisión sobre la admisibilidad de la denuncia.

En el caso de las denuncias inadmitidas, se recogerán todos los datos, salvo aquellos datos que sean datos personales, así como la fecha y hora de introducción de datos en el registro de denuncias, fecha y hora de recepción de la denuncia en el buzón del canal de denuncias, fecha de la decisión sobre la inadmisibilidad de la denuncia y fecha de la eliminación de la denuncia del buzón del canal de denuncias.

Este registro contará con los niveles de protección adecuados para evitar su manipulación y para garantizar la anonimización de los datos personales y un acceso restringido al mismo. Solo podrán introducir datos en el registro y tener acceso al mismo el Responsable del Canal de Denuncias y los usuarios que con roles y accesos limitados hayan sido expresamente designados.

XI.- APROBACIÓN Y ENTRADA EN VIGOR

El órgano de administración de la organización KWD ESPAÑA S.L.U. ha aprobado el presente procedimiento de Canal de Denuncias, con adhesión de los respectivos órganos de gestión de las sociedades filiales.

El procedimiento de Canal de Denuncias entrará en vigor el día siguiente a su publicación en la página web de la organización, teniendo efectos vinculantes para todos los afectados desde esa fecha.

El presente procedimiento será revisado anualmente.

XII.- SEGUIMIENTO, EVALUACIÓN Y REVISIÓN

Se revisará periódicamente y en cualquier caso cuando se produzcan cambios internos o externos a la organización, el procedimiento de gestión, recepción y seguimiento de las informaciones, a los efectos de incorporar actuaciones y buenas prácticas con la finalidad de mejorar el procedimiento.

En función de la revisión y las necesidades o carencias detectadas, se procederá en caso de considerarse necesario a la modificación de este procedimiento, previa aprobación, en su caso por el órgano de administración o de gestión de la organización.

ANEXO I.- INFORMACIÓN SOBRE CANALES EXTERNOS DE INFORMACIÓN.

En cumplimiento de lo dispuesto por la Ley 2/2023 de 20 de febrero, de Protección al Informante, en el ámbito de nuestro **SISTEMA INTERNO DE INFORMACIÓN**, se le informa de los principales canales externos de información a través de los cuales se podrán efectuar igualmente comunicaciones ante las autoridades competentes:

- Autoridad Independiente de Responsabilidad Fiscal: https://www.airef.es/es/canal-de-denuncias/
- Oficina Europea Antifraude: https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_es y https://fns.olaf.europa.eu/main_es.htm
- Canal Externo de la Unión Europea: https://european-union.europa.eu/contact-eu/make-complaint_es
- Infofraude (Hacienda-Gobierno de España): https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/paginas/denan.aspx
- Agencia Tributaria: https://sede.agenciatributaria.gob.es/Sede/colaborar-agencia-tributaria/comunicaciones-ley-2_2023-proteccion-informante-externo/informacion-ley-2_2023-proteccion-informante-externo.html
- Agencia Española de Protección de Datos: https://whistleblowersoftware.com/secure/aepd-canal-proteccion-informante/9950b8af-daf7-493b-92ae-6eb1c7962d99
- Comisión Nacional de los Mercados y la Competencia: https://sede.cnmc.gob.es/tramites/competencia/denuncia-de-conducta-prohibida
- Comisión Nacional del Mercado de Valores: https://www.cnmv.es/portal/whistleblowing/presentacion.aspx
- Banco de España:
- https://www.bde.es/bde/es/secciones/sobreelbanco/Transparencia/Informacion_inst/registro-de- acti/Canal_de_denuncias.html
- Oficina de buenas prácticas y anticorrupción de la comunidad foral de navarra: https://canal.oana.es/

A través de nuestra página web, le informaremos de las actualizaciones que puedan producirse en lo referente a canales externos de información y la creación de canales externos de comunicación de la Autoridad Independiente de Protección al Informante A.A.I.

ANEXO II.- ACTIVIDADES ILÍCITAS

Actividad ilícita es todo comportamiento ilícito y/o ilegal que se encuadre en alguno de los tipos que establece la **Ley Orgánica 10/1995**, de 23 de noviembre, del **Código Penal** y que conllevan la responsabilidad penal de las personas jurídicas, dentro de la cual y para su beneficio se ha llevado a cabo.

Nuestro actual Código Penal contempla un catálogo de delitos que pueden ser aplicables a la organización, junto con aquellos que hayan intervenido, si bien solo parte de ellos tienen alguna probabilidad de llegar a cometerse, dependiendo de nuestra actividad empresarial.

El Sistema Interno de Información debe permitir la recepción de comunicaciones de información relativas a hechos que pudieran suponer, dentro del ámbito de competencias de la organización KDW ESPAÑA S.L.U., las siguientes actividades ilícitas tipificadas en el Código Penal Español como tipos delictivos que conforme al Sistema de Compliance de nuestra organización se consideran de más probable comisión:

a) Descubrimiento y revelación de secretos (art. 197, 197 bis, y 197 ter)
b) Estafa (art. 248 y ss.). Incluida su modalidad agravada, así como la estafa sobre cosa mueble o inmueble y contratos simulados.
c) Frustración de la ejecución (art. 257 y ss.), esto es, alzamiento de bienes, prestación de relación de bienes incompleta o mendaz, uso de bienes embargados sin autorización.
d) Insolvencias punibles (art. 259 y ss.), esto es, disposición de bienes en situación de insolvencia y su modalidad agravada, pago fraudulento a acreedores, prestación de datos contables falsos en procedimiento concursal.
e) Daños informáticos (art. 264, 264 bis y 264 ter).
f) Delitos relativos a la Propiedad Intelectual (art. 270 y 271), incluida su modalidad agravada.
g) Delitos relativos a la Propiedad Industrial (art. 273 y ss.), en concreto, patentes, modelos de utilidad y otros derechos, marcas, nombres comerciales y rótulos de establecimientos. Así como la divulgación de invención objeto de solicitud de patente secreta (art. 277). Quedan excluidas las denominaciones de origen y su modalidad agravada (art. 275 y 276).
h) Apoderamiento, difusión, revelación, cesión, divulgación o utilización de secretos de empresa (art. 278 y ss.), esto es, el apoderamiento de datos u objetos para descubrir un secreto de empresa, la difusión, revelación, cesión o utilización de secreto de empresa por persona obligada a guardar reserva, y el apoderamiento, difusión, revelación, cesión o utilización de un secreto de empresa en cuyo descubrimiento no se ha participado pero con conocimiento de su origen ilícito.
i) Detracción de materias primas o productos de primera necesidad (art. 281).
j) Publicidad engañosa (art. 282).
k) Sociedad emisora de valores negociados, esto es, falsear información económico-financiera (art. 282 bis).
l) Alteración de precios (art. 284).

m) Abuso de información relevante relativa al mercado bursátil y comunicación ilícita de información privilegiada (art. 285, 285 bis, 285 ter y 285 quater).
n) Corrupción en los negocios (art. 286 bis, 286 ter y 286 quater), incluyendo la corrupción entre particulares y la corrupción a funcionario público en actividades económicas internacional.
o) Blanqueo de capitales y sus supuestos agravados (art. 301 y ss.).
p) Financiación ilegal de los partidos políticos (donaciones) (art. 304 bis).
q) Delitos contra la Hacienda Pública y la Seguridad Social (art. 305 y ss.), esto es, el fraude a la Hacienda Pública y sus supuestos agravados, el fraude a los presupuestos generales de la Unión Europea, el fraude a la Seguridad Social y sus supuestos agravados, así como el disfrute indebido de prestaciones del sistema de Seguridad Social (simulación, tergiversación, ocultación), el fraude de ayudas y subvenciones públicas, y el incumplimiento de obligaciones contables establecidas por la ley tributaria.
r) Los delitos contra los derechos de los ciudadanos extranjeros (art. 318 bis).
s) Delitos sobre la ordenación del territorio y el urbanismo (art. 319).
t) Delitos contra los recursos naturales y el medio ambiente (art. 325 y ss.), esto es, emisiones y vertidos, traslado de residuos, explotación de instalaciones con actividades o sustancias peligrosas. Se excluye el daño de espacios naturales protegidos (art 330).
u) Delitos contra la salud pública relacionados con la adulteración de agua o alimentos con sustancias infecciosas u nocivas (art. 365). Quedan excluidas la manipulación de alimentos, adulteración de alimentos con aditivos u otros agentes, adulteración de agua o alimentos con sustancias infecciosas u otras nocivas, la elaboración, suministro, comercialización o despacho, sin autorización, de sustancias nocivas para la salud o productos químicos que puedan causar estragos, así como el despacho o suministro, con autorización pero incumpliendo formalidades legales, de sustancias nocivas para la salud o productos químicos que puedan causar estragos, junto con el despacho o expedición de medicamentos deteriorados, la alteración de medicamentos o sustancias beneficiosas para la salud, y el cultivo, elaboración y tráfico de drogas, estupefacientes y sustancias psicotrópicas.
v) Cohecho activo (art. 424 y ss.), esto es, cometido por particular a autoridades o funcionarios públicos, así como el cometido por particular a autoridades, funcionarios públicos o agentes que trabajen en o para la Unión Europea, u otro país extranjero u organización internacional.
w) Tráfico de influencias (arts. 429 y 430), esto es, el cometido por particular a autoridad o funcionario público, así como el cometido por particular o funcionario público o autoridad (oferta de realizar tráfico de influencias).
x) Malversación (art. 435).
y) Fomento, promoción o incitación al odio, hostilidad, discriminación o violencia contra grupos (art. 510).
z) Organizaciones y grupos terroristas. Delitos de terrorismo. (art. 571 a 580 bis).

Se incluye igualmente el delito de contrabando conforme a lo dispuesto en la ley de represión del contrabando.

Dada nuestra actividad empresarial, se consideran los delitos enumerados a continuación como de baja o nula probabilidad de comisión dentro del ámbito de actuación de nuestra organización:

a) El tráfico ilegal de órganos humanos (art. 156 bis).
b) La trata de seres humanos (art. 177 bis).
c) Los delitos de prostitución (art. 187 y ss.).
d) La facturación de cantidades superiores cuyo coste o precio se mide por aparatos automáticos (art. 283).
e) La usurpación de derechos de emisión y prestación de servicios multimediales (art. 286).
f) Los delitos de riesgo catastrófico (radiaciones y explosivos) (art. 343 y 348), incluida la exposición de personas a radiaciones ionizantes. Queda excluida la contravención de normas de seguridad en la manipulación de explosivos y otros agentes que puedan causar estragos (art. 348).
g) La falsificación de moneda (arts. 386 y 387).
h) La falsificación de tarjetas de crédito, débito o cheques de viaje (art. 399 bis).
i) El cohecho pasivo (art. 419 y ss.), esto es, cometido por autoridad o funcionario público.
j) El tráfico de influencias cometido por autoridad o funcionario público (art. 428).

Asimismo, se consideran actividades contrarias a las Políticas Corporativas de Sistema de Compliance del GRUPO SCHNELLECKE LOGISTICS aplicable a nuestra organización KWD ESPAÑA S.L.U., las relativas al incumplimiento de las obligaciones de los empleados respecto a:

a) Prevención de la corrupción: principios de conducta para el trato con socios comerciales y funcionarios públicos.
b) Conflictos de intereses en la empresa: actividades accesorias, participaciones en empresas y pertenencias a organismos de gestión externos.
c) Ley antimonopolio y de competencia: principios de conducta para una competencia leal.
d) Donaciones y Patrocinios: gestión y ámbitos de financiación admisibles.