



<b>Título de la política:</b> Política del Sistema Interno de Información	<b>Fecha de emisión:</b>
<b>Área funcional:</b> Cumplimiento	<b>Fecha efectiva:</b>
<b>Versión:</b> 1.0	<b>Propietario:</b> Responsable del Sistema Interno de Información- Global Chief Compliance Officer

## POLÍTICA DEL SISTEMA INTERNO DE INFORMACIÓN

### 1.0 INTRODUCCIÓN

De conformidad con lo dispuesto en la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción por la que se transpone la Directiva (UE) 2019/1937 del Parlamento Europeo (en adelante “**Ley 2/2023**”) y en el Código Penal, art.31bis, **OPKO HEALTH EUROPE, S.L.U.**, sus filiales en España (**OPKO HEALTH SPAIN, S.L.U.** y **OPKO LAB EUROPE, S.L.U.**) (colectivamente, “**OPKO SPAIN**”) han procedido a la creación de un Sistema Interno de Información.

La Ley 2/2023 establece en su art.10 que las empresas del sector privado que tengan contratados 50 o más trabajadores están obligadas a disponer de un Sistema Interno de Información

Asimismo, el Código Penal, en el marco de la implementación del Modelo de Prevención de delitos, en su art.31.bis.5. 4º, requiere que se imponga la obligación en las empresas de informar de riesgos e incumplimientos del Modelo de Prevención de Delitos.

Por lo anterior, y dado que el OPKO SPAIN, como compañía del Grupo OPKO, tiene el compromiso de mantener el más alto nivel de estándares profesionales y éticos en la conducción de sus negocios y de crear una cultura empresarial de cumplimiento de la legalidad, se crea el Sistema Interno de Información que se desarrolla en la presente Política.

### 2.0 ÁMBITO DE APLICACIÓN

Es **Responsable del Sistema Interno de Información** objeto de esta Política es Peter Sperger (Global Chief Compliance and Audit Officer / Legal).

Esta Política aplica a todas las sociedades del Grupo OPKO en España, a saber: OPKO HEALTH EUROPE, S.L.U., OPKO HEALTH SPAIN, S.L.U. y OPKO LAB EUROPE, S.L.U.

En este sentido, las referencias a la “**Sociedad**” incluirá a todas y cada una de dichas sociedades y las referencias al “**Grupo**” se entenderá que comprende a todas ellas.

<b>Título de la política:</b> Política del Sistema Interno de Información	<b>Fecha de emisión:</b>
<b>Área funcional:</b> Cumplimiento	<b>Fecha efectiva:</b>
<b>Versión:</b> 1.0	<b>Propietario:</b> Responsable del Sistema Interno de Información

Esta Política es de aplicación y de obligado cumplimiento por parte todas las **“Personas Afectadas**, que incluye:

- Empleados del Grupo.
- Los accionistas, partícipes o personas pertenecientes al Órgano de Administración.
- Profesionales y colaboradores vinculados al Grupo respecto a los que este pueda ostentar, directa o indirectamente, el control.
- Personal en prácticas.
- Representantes contratados (directa o indirectamente) para realizar trabajos para el Grupo incluido el personal de agencias temporales y otros contratistas independientes.

En este sentido, es deber y responsabilidad de todas las **“Personas Afectadas”** que tengan conocimiento o la creencia de buena fe de que una ley, regulación, política o directriz ética aplicable ha sido, está siendo o puede ser violada, informar rápidamente de ello de acuerdo con esta Política.

En especial, son objeto de esta Política y serán tramitadas conforme al procedimiento aquí descrito las siguientes **“Infracciones”**:

- Incumplimiento de normativa interna (Código de Conducta y Manual del Empleado y Políticas de cumplimiento).
- Infracción penal (delitos establecidos en el código penal, como delitos de estafa, fraude a la Hacienda Pública o Seguridad Social, acoso sexual, daños informáticos, blanqueo de capitales o delitos contra la salud pública, entre otros).
- Infracciones administrativas graves o muy graves (solicitud indebida de devoluciones, beneficios o incentivos fiscales, ejercicio de actividades profesionales sin la licencia de actividad pertinente, solicitud de subvenciones de forma fraudulenta o uso y creación de facturas, justificantes u otros documentos análogos falsos, entre otras infracciones). En todo caso, se entenderán comprendidas dentro de este ámbito, las infracciones administrativas que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.
- Cualquier vulneración de la ley.

Cualquier **“Persona Afectada”** que intencionalmente no denuncie, desanime a otra **“Persona Afectada”** de cumplir con su obligación de denunciar, o acose, penalice o tome represalias contra otra **“Persona Afectada”** por cumplir con su obligación de informar, puede estar sujeta a medidas disciplinarias, hasta e incluyendo el despido del empleo.



<b>Título de la política:</b> Política del Sistema Interno de Información	<b>Fecha de emisión:</b>
<b>Área funcional:</b> Cumplimiento	<b>Fecha efectiva:</b>
<b>Versión:</b> 1.0	<b>Propietario:</b> Responsable del Sistema Interno de Información

### **3.0 PROPÓSITO**

Esta Política tiene como objeto establecer el procedimiento de tramitación de las comunicaciones de Infracciones que se reciban, incluyendo las pautas de actuación que deben seguirse desde que se recibe la comunicación de Infracción hasta que se da una resolución a la misma, previa tramitación de la investigación e instrucción.

### **4.0 SISTEMA INTERNO DE INFORMACIÓN**

#### **4.1. Comunicación de una Infracción**

La comunicación de Infracciones puede realizarse de forma escrita o de forma verbal, a través del servicio confidencial de línea directa de terceros mediante:

- Sitio web: [www.lighthouse-services.com/OPKO](http://www.lighthouse-services.com/OPKO)
- Aplicación de denuncia anónima: Palabra clave: OPKO
- Teléfono gratuito: +01 800-603-2869
- Correo electrónico: [reports@lighthouse-services.com](mailto:reports@lighthouse-services.com) (incluya el nombre de OPKO con el informe)

Las Personas Afectadas que elijan hacer llamadas anónimas deben entender que a veces la información proporcionada no es lo suficientemente completa o específica como para realizar una investigación de la Infracción informada, dado que puede resultar necesario contactarles para obtener aclaraciones o información adicional.

Toda comunicación de Infracciones deberá ser interpuesta de buena fe.

Asimismo, el Grupo garantiza que no se adoptarán represalias laborales frente a quienes informen de Infracciones con buena fe, con independencia del acierto indagatorio o preventivo de la misma en términos de veracidad. Tampoco se generará presión, en términos de acoso moral o psicológico, con el objetivo de influenciar en el cese de las acusaciones o como venganza por las mismas. Se trata de un compromiso asumido por el Grupo, mediante la aprobación de esta Política. Esta prohibición y la consiguiente protección del informante por posibles represalias regirá por un periodo de dos años tras la finalización de las diligencias de investigación internas.

<b>Título de la política:</b> Política del Sistema Interno de Información	<b>Fecha de emisión:</b>
<b>Área funcional:</b> Cumplimiento	<b>Fecha efectiva:</b>
<b>Versión:</b> 1.0	<b>Propietario:</b> Responsable del Sistema Interno de Información

De lo contrario, si la información de Infracciones se realiza con mala fe, el Grupo estará habilitado a ejercer las medidas disciplinarias que estime oportunas.

Se considerarán Infracciones realizadas de mala fe aquellas que contengan declaraciones falsas o engañosas, o que omitan intencionalmente hechos que refutarían la creencia de que ha ocurrido una Infracción.

#### **4.2. Contenido de la comunicación de Infracción**

El contenido de la comunicación de Infracción debe ser el siguiente:

- Identificación del informante (nombre completo, DNI, correo electrónico y vinculación con el Grupo) o marcar la opción anónimo.
- Identificación del departamento y/o actividad dónde se han producido los hechos o dónde se ha tenido conocimiento de los indicios referenciados.
- Nombre de la persona/s investigada o delimitación del área (si se conoce).
- Descripción de los hechos y circunstancias en las que ocurrieron.
- Todos los medios de prueba al alcance del informante que sean relevantes, oportunos y lícitos.
- Fecha en la que se produjeron los hechos.
- Personas que han presenciado o tienen conocimiento de los hechos.
- Cómo se ha tenido conocimiento del hecho comunicado.

#### **4.3. Tramitación del procedimiento**

**4.3.1. (registro)** Lighthouse Services recibirá la comunicación de Infracción y procederá a su registro (con todos los datos aportados por el informante), asignándole un número de referencia, donde recogerá todas las actuaciones que lleve a cabo al respecto, si bien no se incluirán datos personales.

Lighthouse Services proporcionará al informante el número de registro del expediente.

El Responsable del Sistema Interno de Información y el/los *Compliance Officer(s)* tendrán acceso a dicho registro así como al contenido de las actuaciones realizadas.

Tanto el informante como la persona investigada podrán consultar el estado de la tramitación del expediente (no su contenido).

<b>Título de la política:</b> Política del Sistema Interno de Información	<b>Fecha de emisión:</b>
<b>Área funcional:</b> Cumplimiento	<b>Fecha efectiva:</b>
<b>Versión:</b> 1.0	<b>Propietario:</b> Responsable del Sistema Interno de Información

La información indicada quedará almacenada de forma indefinida en el sistema con el objetivo de acreditar el funcionamiento del sistema ante una posible investigación judicial.

**4.3.2. (acuse de recibo)** Lighthouse Services dispondrá del plazo de 7 días naturales para remitir un acuse de recibo al informante, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.

**4.3.3. (validación)** Lighthouse Services validará la comunicación de Infracción, esto es, validará que se refiera a incumplimientos que se enmarcan en el ámbito de la presente Política (infracciones indicadas en el punto 2.0), y que tienen fundamento suficiente para ser tramitada.

En el caso de que la comunicación de Infracción se refiera a hechos que quedan fuera del ámbito objetivo de esta Política o que carezcan manifiestamente de fundamento, dicha no validación será comunicada al informante y se procederá al archivo de la comunicación de Infracción.

**4.3.4. (tramitación)** Lighthouse Services comunicará la comunicación de Infracción al Responsable del Sistema Interno de Información, siempre que no exista incompatibilidad o un conflicto de intereses con éste.

El Responsable del Sistema Interno de Información nombrará un **Responsable de la Investigación**, para coordinar la tramitación del expediente.

El Responsable de la Investigación llevará a cabo las actuaciones que considere necesarias para tramitar la instrucción del expediente. Para ello podrá recabar toda la información y documentación que considere necesaria de cualquier área, división o departamento, respetando siempre los derechos fundamentales de la/s persona/s que sean objeto de investigación.

En este sentido, durante la instrucción del expediente, el Responsable de la Investigación podrá mantener comunicación con el informante y, si lo considera necesario, solicitarle información adicional.

El Responsable de la Investigación podrá nombrar a un equipo para la instrucción del expediente, que podrá estar formado por:

- uno o varios *Compliance Officer(s)* con quienes no exista incompatibilidad o un conflicto de intereses.
- Una o varias Personas Afectadas que se consideren competentes.

<b>Título de la política:</b> Política del Sistema Interno de Información	<b>Fecha de emisión:</b>
<b>Área funcional:</b> Cumplimiento	<b>Fecha efectiva:</b>
<b>Versión:</b> 1.0	<b>Propietario:</b> Responsable del Sistema Interno de Información

- Uno o varios expertos o asesores externos.

**4.3.5. (duración)** La duración máxima de las actuaciones de investigación / instrucción será de tres meses desde el acuse de recibo remitido conforme a lo indicado en el apartado 4.3.2 anterior o, si no se remitió acuse de recibo, desde la finalización del plazo de siete días concedido para ello. En casos de especial complejidad, que deberán justificarse por escrito por parte del Responsable de la Investigación, podrá ampliarse el plazo por tres meses adicionales.

**4.3.6. (resolución)** Concluida la investigación, el Responsable de la Investigación realizará un informe que compartirá con el Responsable del Sistema Interno de Información para su aprobación.

**4.3.7. (ejecución de medidas)** Será decisión del Responsable del Sistema Interno de Información establecer las medidas a adoptar para la resolución del expediente, todo ello, tras la consulta del informe elaborado por el Responsable de la Investigación y aprobado por el Responsable del Sistema Interno de Información.

Asimismo, se remitirá al Ministerio Fiscal con carácter inmediato el informe en cuestión cuando los hechos pudieran ser indiciariamente constitutivos de delito.

**4.3.8. (comunicación al informante)** Aprobado el informe y adoptadas, en su caso, las medidas correspondientes, se comunicará al informante que la tramitación de la comunicación de Infracción ha concluido y que se procederá al archivo de la misma.

**4.3.9. (archivo)** Tras la comunicación al Informante y, en su caso, al Ministerio Fiscal, el expediente será archivado.

## **5.0 DERECHOS, PRINCIPIOS y GARANTÍAS**

### **5.1. Derechos del informante**

El informante tendrá derecho a:

- Decidir si desea realizar la comunicación de Infracción forma anónima o no.
- Formular la comunicación verbalmente o por escrito.
- Indicar un lugar donde recibir las comunicaciones.
- Renunciar a su derecho a recibir comunicaciones.

<b>Título de la política:</b> Política del Sistema Interno de Información	<b>Fecha de emisión:</b>
<b>Área funcional:</b> Cumplimiento	<b>Fecha efectiva:</b>
<b>Versión:</b> 1.0	<b>Propietario:</b> Responsable del Sistema Interno de Información

- Comparecer ante el Responsable del Sistema Interno de Información, el Responsable de la Investigación y/o el/los *Compliance Officer(s)* si lo considera oportuno.
- Solicitar que la comparecencia sea realizada por videoconferencia u otros medios telemáticos.
- Ejercer los derechos que confiere la legislación en materia de protección de datos de carácter personal.
- Comunicar a través del Canal Externo de Información gestionado por parte de la Autoridad Independiente de Protección de Informante cualesquiera acciones u omisiones incluidas en el ámbito de ampliación de esta Política y de la Ley 2/2023, ya sea directamente o previa comunicación a través del Sistema Interno de Información del Grupo.

## **5.2. Derechos de las personas investigadas**

La persona investigada tiene derecho a la presunción de inocencia, derecho al honor, al derecho de defensa, de ser informado de las acciones u omisiones que se le atribuyen, a ser oída en cualquier momento, debiendo tener acceso al expediente durante la tramitación del mismo.

Asimismo, las personas investigadas tendrán derecho a la misma protección establecida en esta Política para los informantes en relación con la preservación de su identidad y la confidencialidad de los hechos y datos del expediente.

El acceso al expediente por parte de la persona investigada será en relación con los hechos que sean objeto de investigación, sin que sea posible un acceso que le permita identificar al informante o a los terceros que se mencionen en el expediente.

El Responsable del Sistema Interno de Información decidirá qué documentos e información es posible compartir con la persona investigada en caso de que lo solicite.

## **5.3. Principios y garantías**

Todos las Personas Afectadas tienen el derecho y la obligación de comunicar Infracciones.

El acceso al Sistema Interno de Información por parte de las Personas Afectadas como incentivo para el cumplimiento de su deber de comunicación de Infracciones lleva aparejada la necesidad de proteger al informante.

<b>Título de la política:</b> Política del Sistema Interno de Información	<b>Fecha de emisión:</b>
<b>Área funcional:</b> Cumplimiento	<b>Fecha efectiva:</b>
<b>Versión:</b> 1.0	<b>Propietario:</b> Responsable del Sistema Interno de Información

Para ello, se aplicarán las garantías de:

**5.3.1. (autonomía e independencia de los intervinientes en el Sistema Interno de Información)** Tanto Lighthouse Services, como el Responsable del Sistema Interno de Información, el/los *Compliance Officer(s)* y el Responsable de la Investigación tienen garantizada su autonomía mediante designación formal por el órgano de administración del Grupo, por lo que se comprometen a velar por la confidencialidad y protección del informante sin admitir presiones ni injerencias de ningún tipo u origen.

**5.3.2. (confidencialidad y secretos de las comunicaciones)** Se garantiza la confidencialidad tanto del expediente como de la identidad de las personas implicadas. En este sentido, todos los informes se mantendrán confidenciales, se solicite dicha confidencialidad o no, con el fin de impedir tanto la revelación de datos de carácter personal, como cualquier detalle que permita la identificación de las personas implicadas.

La identidad de las personas implicadas únicamente 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.

**5.3.3. (prohibición de represalias)** Ningún informante será penalizado u objeto de represalias por comunicar de buena fe de cualquier sospecha de Infracción. Esta protección también se extiende a las personas afectadas que proporcionen información como parte de la instrucción de un expediente.

Los gerentes y supervisores deben asegurarse de que las Personas Afectadas no estén sujetas a consecuencias adversas porque hayan cuestionado una práctica del Grupo.

Cualquier Persona Afectada que acose o tome represalias contra otra Persona Afectada que de buena fe comunique una Infracción (o una sospecha de Infracción), podrá ser sancionada disciplinariamente.

**5.3.4. (protección del informante)** Los participantes en el Sistema Interno de Información serán los encargados de velar por la protección del informante, garantizando la no revelación de su identidad y datos personales, así como la ausencia de represalias. En caso de que se requiera al informante para la aportación de datos o testimonios adicionales de cara a observar la veracidad y gravedad de la comunicación realizada, habrá de hacerse garantizando que tanto en el requerimiento como en la respuesta se mantengan los niveles de protección antedichos.

<b>Título de la política:</b> Política del Sistema Interno de Información	<b>Fecha de emisión:</b>
<b>Área funcional:</b> Cumplimiento	<b>Fecha efectiva:</b>
<b>Versión:</b> 1.0	<b>Propietario:</b> Responsable del Sistema Interno de Información

**5.3.5. (ausencia de conflicto de interés)** No formará parte de la tramitación e investigación de la comunicación de Infracción ninguna persona relacionada con la misma.

En la toma de decisiones para la resolución de la comunicación de Infracción deberán inhibirse las personas afectadas por la misma.

## **6.0 TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL**

El tratamiento de datos personales que deriven de la aplicación de esta Política se regirán por lo dispuesto en la siguiente normativa:

- el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016;
- la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantías de los derechos digitales;
- 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
- el TÍTULO VI 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 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.

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.

Se trata de un tratamiento que pretende cumplir con una obligación legal y al mismo tiempo atender un interés vital de los informantes de Infracciones, por lo que estaría amparado por lo previsto en los siguientes artículos:

- 6.1.c) del Reglamento (UE) 2016/679,
- 8 de la Ley Orgánica 3/2018; y
- 11 de la Ley Orgánica 7/2021: y
- artículos 10 y 13 de la Ley 2/2023.

Los interesados pueden ejercer los derechos recogidos en los art. 11 a 22 del Reglamento (UE) 2016/679. En concreto, los interesados podrán ejercitar su (i) derecho de acceso, (ii) derecho de rectificación, (iii)

<b>Título de la política:</b> Política del Sistema Interno de Información	<b>Fecha de emisión:</b>
<b>Área funcional:</b> Cumplimiento	<b>Fecha efectiva:</b>
<b>Versión:</b> 1.0	<b>Propietario:</b> Responsable del Sistema Interno de Información

derecho de supresión, (iv) derecho de oposición, (v) derecho a la limitación, y, (vi) derecho a la portabilidad de sus datos mediante un escrito identificado con la referencia “Protección de Datos”, acompañando su DNI o documento equivalente, por las dos caras, dirigido al Responsable del Tratamiento de los datos, esto es el Grupo, a través del correo electrónico [ProteccionDeDatos.Spain@opko.com](mailto:ProteccionDeDatos.Spain@opko.com).

No obstante lo anterior, en caso de que la persona a la que se refieren los hechos relatados en la comunicación ejerciera el derecho de oposición se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales.

El acceso a los datos e carácter personal contenidos en el registro del Sistema Interno de Información quedará limitado a:

- El Grupo, como Responsable del Tratamiento de los datos.
- El Responsable del Sistema Interno de Información
- El Responsable de la Investigación.
- El/los *Compliance Officer(s)*.
- En su caso, el Responsable de RRHH del Grupo.
- El Responsable de los servicios jurídicos, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.
- Los encargados del tratamiento que eventualmente se designen.

El tratamiento de datos tendrá el siguiente alcance:

- Registro de las comunicaciones de Infracciones recibidas.
- Conservación de los datos personales recibidos. El plazo de conservación de los datos personales recibidos será el estrictamente imprescindible para decidir sobre la procedencia de iniciar una investigación que no podrá superar en ningún caso, los diez años, de conformidad con lo dispuesto en el artículo 26.2 de la Ley 2/2023, de 20 de febrero.
- Supresión de los datos personales recibidos en los siguientes casos:
  - Transcurridos tres meses desde la recepción de la comunicación sin que se hubiese iniciado actuaciones de investigación, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del Sistema Interno de Información.
  - Cuando los datos se refieran a conductas que no consistan en ningún tipo de Infracción.
  - Cuando la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos.



<b>Título de la política:</b> Política del Sistema Interno de Información	<b>Fecha de emisión:</b>
<b>Área funcional:</b> Cumplimiento	<b>Fecha efectiva:</b>
<b>Versión:</b> 1.0	<b>Propietario:</b> Responsable del Sistema Interno de Información

- Si se acreditara que la información facilitada o parte de ella no es veraz, 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.

Todos los datos serán tratados con la más estricta confidencialidad, únicamente por el personal autorizado para ello y con la única finalidad de investigar, tramitar y, en su caso, resolver la posible incidencia o irregularidad comunicada.

En el tratamiento de datos personales derivado de la presente Política intervendrá personal de la sociedad matriz del Grupo OPKO (Opko Health Inc.) así como terceros Lighthouse Services (ubicados, en ambos casos, en EEUU) quienes actuarán como Encargados del Tratamiento y con quienes se han establecido unos procedimientos de trabajo y una distribución de tareas y responsabilidades de forma que se garantiza disponer y aplicar medidas de seguridad adecuadas y suficientes para el tratamiento de los datos personales.

Existe por tanto una posible transferencia internacional de datos, si bien el informante puede optar por mantener su anonimato y, en caso de facilitar sus datos, se le informará oportunamente del contenido del artículo 13 del Reglamento (UE) 2016/679 y del artículo 11 de la Ley Orgánica 3/2018.

## **7.0 PROPIEDAD DE LA POLÍTICA**

Esta Política es propiedad del Responsable del Sistema Interno de Información y no se pueden realizar cambios a menos que se cuente con la autorización expresa y previa del Responsable del Sistema Interno de Información, que debe rastrearse adecuadamente en el Registro de seguimiento de documentos, a continuación.

<b>Versión</b>	<b>Evento / Cambio</b>	<b>Redactado por</b>	<b>Aprobador</b>	<b>Fecha de entrada en vigor</b>
1.0	Redacción de la Política			