Política General del Sistema Interno de Información y Defensa del Informante

Versión 1.0

España



ÍNDICE

1 INTRODUCCIÓN 3

2 PRINCIPIOS DE ACTUACIÓN Y GARANTÍAS ESENCIALES ¡Error! Marcador no definido.

3 RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN 4

4 AUTORIDAD INDEPENDIENTE DE PROTECCIÓN DEL INFORMANTE (AIPI) 4

5 CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES 5

6 MEDIDAS DE PROTECCIÓN 5

7 RÉGIMEN DISCIPLINARIO 7

8 PUBLICIDAD, REVISIÓN Y ACTUALIZACIÓN 8

9 CANALES INTERNOS DE INFORMACIÓN 8

ANEXO I CANALES EXTERNOS DE INFORMACIÓN AUTONÓMICOS 12

1 INTRODUCCIÓN

La transposición de la Directiva (UE) 2019/1937 al ordenamiento jurídico español, mediante la Ley 2/2023, de 20 de febrero, ha establecido un marco específico para garantizar que las personas que tengan conocimiento de posibles irregularidades puedan comunicarlas de forma segura y con plena protección.

En este contexto, SMITH NEPHEW, S.A.U. ha implantado un Sistema Interno de Información (SIIF) como herramienta clave de supervisión, control y prevención en materia de cumplimiento normativo, configurándose como el cauce preferente para la comunicación de posibles incumplimientos.

Si bien la organización dispone de un marco corporativo global en materia de *whistleblowing*, la presente Política se aprueba específicamente para su aplicación en España, con el fin de dar cumplimiento a las exigencias previstas en la normativa nacional y adaptar dicho marco a las particularidades legales y operativas del ordenamiento jurídico español.

El SIIF integra canales internos y externos gestionados con garantías de confidencialidad, independencia y cumplimiento normativo, incluyendo la protección de datos personales, y asegura principios esenciales como el anonimato —cuando proceda—, la integridad de la información, la protección de la persona informante y la prohibición de represalias.

La presente Política, junto con el procedimiento de gestión de las comunicaciones, establece los principios y garantías del Sistema Interno de Información, constituyendo un elemento esencial para su adecuado funcionamiento en España.

2 PRINCIPIOS DE ACTUACIÓN Y GARANTÍAS ESENCIALES

El Sistema Interno de Información (SIIF) constituye uno de los ejes esenciales del sistema de cumplimiento normativo y prevención penal de la Entidad. En línea con las directrices corporativas globales en materia de *whistleblowing*, y con el apoyo de BONET Consulting para garantizar su plena adecuación a la normativa española, la Entidad ha dotado al SIIF de las garantías necesarias para asegurar su eficacia:

- **Independencia, imparcialidad y ausencia de conflictos de interés**: Las comunicaciones se gestionan mediante mecanismos que garantizan un análisis objetivo e independiente, evitando cualquier interferencia o conflicto en su tratamiento.
- **Profesionalidad y diligencia**: La gestión del sistema se encomienda a personas con experiencia en cumplimiento normativo, asegurando una tramitación rigurosa y respetuosa con los derechos de todas las personas implicadas.
- **Confidencialidad, protección de datos y secreto**: Se garantiza la confidencialidad de la información, el acceso restringido a personal autorizado y el cumplimiento de la normativa en materia de protección de datos personales en todas las fases del proceso.
- **Anonimato y accesibilidad del sistema**: El SIIF permite la presentación de comunicaciones anónimas —cuando proceda— y se configura como un canal accesible, sencillo y gratuito para todas las personas legitimadas.
- **Registro y trazabilidad de la información**: Las comunicaciones y actuaciones derivadas son debidamente registradas y conservadas de forma segura, garantizando su integridad y adecuada gestión conforme a la normativa aplicable.
- **Investigación diligente y protección de las personas**: Las comunicaciones son objeto de análisis e investigación conforme a procedimientos internos definidos, garantizando la protección tanto de la persona informante como de las personas afectadas, así como la prohibición de represalias.

- **Buena fe en el uso del sistema**: El uso del SIIF debe realizarse de forma responsable y de buena fe, pudiendo derivarse medidas disciplinarias en caso de comunicaciones falsas o realizadas con carácter malicioso.

3 RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN

Para garantizar la eficacia del Sistema Interno de Información (SIIF), resulta imprescindible la designación de una o varias personas responsables de su correcto funcionamiento, organización y tramitación diligente de las comunicaciones, así como de su adecuada difusión y del desarrollo y actualización del correspondiente plan de formación.

A estos efectos, el órgano de administración u órgano de gobierno de la Entidad ha designado, a nivel local en España, a las personas responsables del Sistema Interno de Información, pertenecientes, respectivamente, a los departamentos de Compliance y de Personas de la Entidad, siendo igualmente competente para su comunicación a la autoridad correspondiente, así como para su eventual cese o sustitución (en adelante, las personas responsables del Sistema).

Las personas responsables del Sistema ejercerán sus funciones con plena independencia y autonomía respecto del resto de órganos de la Entidad, evitando cualquier situación de conflicto de interés. No obstante, podrán contar con el apoyo de terceros o de otras áreas internas para disponer de asesoramiento especializado o reforzar las garantías de independencia en el desempeño de sus funciones.

En particular, para el adecuado ejercicio de sus funciones, las personas responsables del Sistema podrán coordinarse con los siguientes sujetos:

A. El responsable de recursos humanos, cuando pudiera proceder la adopción de medidas disciplinarias contra las personas implicadas y/o coordinar la aplicación de medidas de protección.

B. Los responsables de cumplimiento normativo y/o de los servicios jurídicos de la Entidad, si procediera la adopción de medidas de carácter legal o de cumplimiento normativo que deben ser tomadas en consideración, por estos, en relación con las comunicaciones recibidas en el SIIF.

C. Los encargados del tratamiento que eventualmente se designen.

D. El Delegado / Responsable de Protección de Datos.

E. Otras personas y/o entidades intervinientes en la gestión del SIIF.

4 AUTORIDAD INDEPENDIENTE DE PROTECCIÓN DEL INFORMANTE (AIPI)

El **Sistema Interno de Información (SIIF)** de la Entidad es el medio prioritario y de utilización obligatoria para la comunicación de conductas ilícitas o infracciones de las que se tenga conocimiento, pues permite asegurar la debida adopción de medidas de protección y fomentar la cultura de la información dentro de la organización.

No obstante, se han determinado otros canales de información "externos", con el fin de ofrecer a los ciudadanos una alternativa donde presentar la comunicación y/o reclamación, en los supuestos que los canales internos no cumplan con las garantías exigidas por la normativa aplicable, no se apliquen las pertinentes medidas de protección o las personas sean expuestas a represalias por su condición de informantes.

Por consiguiente, las personas que en el contexto de su relación laboral o profesional hayan tenido conocimiento de infracciones del derecho de la Unión Europea, de delitos o de infracciones

administrativas graves o muy graves pueden informar directamente a la Autoridad Independiente de Protección del Informante (AIPI), Autoridad estatal, a través de las siguientes vías:

- Buzón de denuncias anónimas:

  https://whistleblowersoftware.com/secure/canal_externo_de_denuncias_AINPI

- Correo electrónico: canal.externo@proteccioninformante.es
- Mediante correo postal (Autoridad Independiente de Protección del Informante, Calle Luis Cabrera 9, 28002 Madrid).
- Solicitando una reunión presencial.

En el siguiente enlace se establecen las indicaciones de uso de los canales de la Autoridad estatal: https://www.proteccioninformante.gob.es/como-presentar-la-denuncia

Además, junto a la Autoridad estatal, existen autoridades autonómicas a las que se han atribuido competencias para actuar como canales externos en su ámbito territorial. Se adjunta como ANEXO I la relación de autoridades autonómicas con sus respectivos accesos a los canales externos de información habilitados.

5 CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES

Los tratamientos de datos personales que derivan del Sistema Interno de Información (SIIF) se rigen 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 y en la Ley Orgánica 7/2021, de 26 de mayo. Por ello, en el momento de la captación, los interesados son informados del tratamiento de sus datos y de sus derechos, de acuerdo con la normativa vigente.

En cumplimiento del principio de minimización de datos, los datos de carácter personal recopilados son aquellos necesarios y pertinentes para el tratamiento de la comunicación. En el supuesto de que se recopilen datos por accidente, que no sean necesarios para el conocimiento e investigación de las acciones u omisiones, estos serán eliminados sin dilación indebida. Asimismo, los datos se conservarán durante el tiempo imprescindible para decidir sobre la precedencia de iniciar una investigación.

Por otro lado, el diseño del SIIF garantiza la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, así como de las actuaciones desarrolladas en la gestión y tramitación de la misma. En este sentido, el acceso a los datos personales y el resto de información contenida en el sistema está limitada a los responsables de la gestión, dentro del ámbito de sus competencias y funciones. Por lo tanto, se dispone de medidas técnicas y organizativas adecuadas para preservar la identidad de los afectados e impedir el acceso de personas no autorizadas.

En el caso de cualquier duda o consulta sobre el tratamiento de datos de carácter personal llevado a cabo en el seno de la Entidad en relación con el SIIF, todo interesado puede dirigirse al Delegado / Responsable de Protección de Datos designado a través de la siguiente dirección de correo electrónico: privacy@smithnephew.com

6 MEDIDAS DE PROTECCIÓN

Las personas que comuniquen o revelen infracciones utilizando el Sistema Interno de Información (SIIF) de la Entidad tienen derecho a protección, en las mismas condiciones que quienes informen por canales externos, siempre que 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.

En este sentido, se prohíben expresamente los actos constitutivos de represalia, incluida la amenaza y tentativa, contra las personas que presenten una comunicación. Se entiende por represalia:

a) Actos u omisiones prohibidos por la ley.

b) Actos u omisiones que de forma directa o indirecta supongan un trato desfavorable, situando a la persona en desventaja con respecto a otra.

A título enunciativo y no limitativo, se consideran represalias:

- Suspensión del contrato de trabajo, despido o extinción de la relación, terminación anticipada, anulación del contrato de trabajo y/o mercantil, medidas disciplinarias, amonestación u otra sanción, degradación o denegación de ascensos, modificación sustancial de las condiciones y no conversión del contrato temporal en indefinido o medidas equivalentes.
- Daños (incluidos reputacionales), pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.
- Evaluación o referencias negativas sobre el desempeño laboral o profesional.
- Listas negras o difusión de información que dificulte o impida el acceso a empleo / contratos de obras o servicios.
- Denegación o anulación de licencia o permiso.
- Denegación de formación.
- Discriminación, trato desfavorable o injusto.
- Denegación de incentivos, beneficios, bonos, comisiones y cualquier otro tipo de compensación.
- Terminación anticipada, suspensión, alteración o anulación de contratos de bienes o servicios.

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 al perjudicado.

A efectos de garantizar el derecho de protección del informante y el de las personas afectadas por la comunicación, la Entidad tiene establecidas las siguientes medidas técnicas y organizativas las cuales se aplican desde el momento inicial en el que se recibe la comunicación:

- **Configuración del SIIF**: El SIIF se ha diseñado con las medidas técnicas y organizativas adecuadas para garantizar la protección de la identidad del informante, así como de aquellos datos e informaciones que se deriven de las comunicaciones presentadas. En este sentido, la Entidad ha habilitado una serie de canales internos de información, los cuales permiten presentar comunicaciones de forma anónima. Dichos canales son:
  - **Canal on-line / digital**: Plataforma digital "SpeakUp" habilitada para la presentación de comunicaciones por escrito. Su funcionamiento operativo, así como la trazabilidad de las informaciones comunicadas, se encuentran debidamente regulados en el Procedimiento de Gestión de Informaciones de la Entidad.
  - **Canal telefónico**: Integrado en la plataforma "SpeakUp" de la Entidad, este canal permite la presentación de comunicaciones en distintos idiomas, en función de las necesidades de la persona informante.
  - **Canal presencial / "face to face"**: El Sistema de recepción de comunicaciones mediante reunión presencial o por videoconferencia. Esta vía cuenta con el soporte del experto externo BONET consulting, otorgando altos estándares de cumplimiento.

  Con independencia del canal que se utilice, el SIIF garantiza la aplicación efectiva de los principios básicos y garantías especificadas en la presente Política, a fin de cumplir con los requisitos del marco normativo y proteger los derechos de los informantes y las personas afectadas.

- **Responsable del SIIF**: Para asegurar la debida aplicación del SIIF, la Entidad tiene designadas a las personas responsables del Sistema, pertenecientes, respectivamente, a los departamentos de Compliance y de Personas de la Entidad, cuyas funciones radican en la supervisión, vigilancia y control de su correcto funcionamiento. En este sentido, dichas personas responsables, junto con el experto externo, adoptarán las medidas de protección necesarias y velarán por el adecuado seguimiento y aplicación del Sistema. La participación del experto externo dota a las funciones atribuidas a las personas responsables del Sistema de los elementos de autonomía e independencia requeridos por la normativa vigente.

  Asimismo, en aquellos supuestos en los que las personas responsables del Sistema, como consecuencia de ocupar simultáneamente otras posiciones o funciones dentro de la organización, tuvieran conocimiento de una posible irregularidad o de una comunicación trasladada informalmente por una persona trabajadora o tercero, deberán remitir a la potencial persona informante a los canales internos de información debidamente habilitados por la Entidad. Todo ello, con la finalidad de garantizar la adecuada confidencialidad, la debida protección de datos personales y el funcionamiento profesional, trazable y conforme a derecho del Sistema Interno de Información.

  Igualmente, las personas responsables del Sistema serán las encargadas de realizar un análisis preliminar de las comunicaciones recibidas, a efectos de determinar la idoneidad de adoptar medidas de protección específicas respecto de la persona informante y/o de terceros afectados. Además, en función de la naturaleza y alcance de la información recibida, contarán con el apoyo y asesoramiento de las personas responsables de las diferentes áreas operativas de la Entidad, para el adecuado desarrollo de las actuaciones de investigación. Del mismo modo, podrán recurrir a terceros especializados en aquellas materias que requieran una valoración técnica o experta.

- **Custodia, gestión y seguridad de la información del SIIF**: La Entidad dispone de un sistema de gestión documental configurado con las medidas apropiadas de seguridad y control, a efectos de evidenciar la propia eficacia del SIIF. Cabe destacar que dicho sistema incluye procesos de anonimización, a fin de no permitir la identificación de los informantes. Adicionalmente, la Entidad ha adoptado medidas técnicas razonables para la conservación, recuperación y eliminación de manera segura de la información, así como la implantación de controles de acceso para impedir el uso no autorizado.

Sin embargo, quedan excluidas de la mencionada protección las informaciones remitidas que sean falsas, tergiversadas, carezcan manifiestamente de toda verosimilitud y fundamento o existan indicios racionales de haberse obtenido mediante la comisión de un delito. Esto es debido a que todas las comunicaciones deben realizarse bajo el principio de buena fe y, por tanto, el informante debe tener motivos razonables para pensar que la información es veraz en el momento de la comunicación. En resumen, el principio de buena fe requiere que en ningún caso pueda desprenderse que existe falsedad, falta a la verdad, intención de venganza o de perjudicar a un tercero.

Es importante recordar que las medidas de protección no se dirigen sólo a favor de los informantes. También aquellas personas a las que se refieran los hechos relatados en la comunicación (personas afectadas) cuentan con una singular protección ante el riesgo de que la información, aún con aparentes visos de veracidad, haya sido manipulada, sea falsa o responda a otras motivaciones. Durante la tramitación del expediente, estas personas tienen derecho a la presunción de inocencia, a la tutela judicial y defensa, al acceso al expediente, así como a la confidencialidad de los hechos y datos del procedimiento y a la reserva de su identidad. En conclusión, tienen la misma protección y derechos que goza el informante.

7 RÉGIMEN DISCIPLINARIO

El incumplimiento de la normativa aplicable y las conductas contrarias a las instrucciones, políticas, códigos, procedimientos y protocolos de la Entidad es motivo de aplicación del régimen disciplinario a

nivel laboral y mercantil, en coordinación con lo establecido en el Convenio Colectivo de aplicación, el Estatuto de los Trabajadores y el resto de las normas aplicables.

La Entidad notificará y sancionará las acciones u omisiones contrarias a la presente Política en las que incurran los empleados, colaboradores o cualquier miembro relacionado con la Entidad y, en particular:

- La no comunicación de cualquier sospecha o conocimiento de infracciones e incumplimientos del marco normativo y de los protocolos y normas internas de la Entidad a través del SIIF.
- Cualquier intento o acción efectiva de obstaculizar la presentación de comunicaciones o impedir, frustrar o ralentizar su seguimiento.
- La utilización del SIIF de mala fe, por ejemplo, con la aportación de información o documentación a sabiendas de su falsedad.
- La adopción de cualquier represalia derivada de la comunicación frente a los informantes o las demás personas afectadas.
- La vulneración de las garantías de confidencialidad y anonimato, revelando la identidad de las personas afectados y quebrantando el deber de secreto de las informaciones.
- El incumplimiento de la obligación de colaboración con la investigación de informaciones.

8 COMUNICACIÓN, REVISIÓN Y ACTUALIZACIÓN

La presente Política, así como toda la información necesaria sobre el uso del Sistema Interno de Información (SIIF) implantado, está disponible en una sección separada y rápidamente identificable, para que todos los interesados la tengan a su alcance de forma clara y fácilmente accesible. No obstante, cualquier persona puede solicitar información adicional a la Entidad a través de los datos de contacto del Responsable.

Las personas Responsables del Sistema revisará periódicamente y, en su caso, propondrá al órgano de administración u órgano de gobierno de la Entidad la actualización de la presente Política, con la finalidad de adaptarla a todas aquellas circunstancias y cambios que puedan ir surgiendo, así como a la normativa o jurisprudencia que pueda dictarse. Todo ello, con el objetivo de adecuar el SIIF a las máximas exigencias de cumplimiento normativo para su correcto funcionamiento y eficacia.

Asimismo, la Entidad está abierta a cualquier sugerencia y/o propuesta que pueda mejorar su actuación ética y favorecer una cultura de cumplimiento normativo, remarcando la necesidad de que todos los empleados y miembros relacionados con la Entidad o terceros colaboren para cumplir con sus valores y principios.

9 CANALES INTERNOS DE INFORMACIÓN

A efectos de cumplir con las disposiciones recogidas en la Ley 2/2023, la Entidad tiene implementado un sistema configurado con los requisitos técnicos y procedimentales requeridos por dicha Ley para la debida atención de las comunicaciones. Todo ello con la finalidad de ofrecer a los informantes un entorno de comunicación seguro, confidencial o incluso anónimo con la Entidad, y tramitar las informaciones de forma eficiente, profesional e independiente.

Para ello, la Entidad se ha dotado de recursos materiales, técnicos y humanos para habilitar distintos canales internos que permiten la presentación de comunicaciones en formato escrito o verbal. Dichos canales cuentan con la configuración, diseño y soporte de un experto externo en aras de aportar los más altos niveles de profesionalidad, experiencia, independencia, confidencialidad, protección de datos y del informante, y otros ámbitos aplicables para este tipo de canales.

Cabe destacar que, la información proporcionada mediante cualquiera de los canales internos será tratada de manera confidencial, y solo tendrá acceso a la misma el personal autorizado para su debida gestión y tramitación.

A continuación, se detallan los canales de los que dispone cualquier empleado o tercero vinculado con la Entidad para la presentación de las comunicaciones.

Canal On-line/Digital

La Entidad dispone de una herramienta digital, gestionada por "Convercent", que permite la presentación de comunicaciones por escrito a través de la plataforma "SpeakUp". El link de acceso es el siguiente: **http://www.speakup.smith-nephew.com/**

Dentro de dicha plataforma, el acceso al apartado "Report an Incident" (reportar un incidente) requiere que la persona informante indique, en primer lugar, su localización y la del suceso comunicado. A continuación, se accede a una nueva pantalla en la que deberá aceptarse un aviso informativo ("pop-up") sobre las características y condiciones de uso del sistema. Una vez aceptado, la herramienta permite seleccionar el idioma de utilización entre múltiples opciones disponibles.

Posteriormente, la plataforma guía a la persona informante en la cumplimentación de la comunicación, solicitando información estructurada que incluye, entre otros aspectos: la descripción de los hechos y las personas implicadas; la fecha y ubicación en la que se produjeron; la posibilidad de adjuntar documentos o evidencias; así como la indicación de si la comunicación se realiza de forma nominativa o anónima y la relación de la persona informante con la Entidad (persona empleada, exempleada, tercero, entre otros).

Completada la información, el sistema solicita la creación de una contraseña que permitirá a la persona informante acceder posteriormente a la plataforma para consultar el estado de su comunicación y mantener, en su caso, la interlocución con las personas Responsables del Sistema, incluso en supuestos de anonimato.

La herramienta cuenta con medidas de seguridad que garantizan la protección de la información, la confidencialidad del proceso y la identidad de las personas intervinientes, asegurando un entorno seguro para la recepción y gestión de las comunicaciones. El acceso a la plataforma se encuentra disponible a través de la página web de la Entidad

Canal telefónico

En la misma herramienta digital, gestionada por "Convercent", se habilita una funcionalidad específica denominada "Call Us", que permite a la persona informante optar por la comunicación telefónica como vía alternativa a la presentación escrita de la comunicación.

Para su utilización, la persona informante deberá seleccionar, mediante un desplegable, el país desde el que realiza la llamada, lo que permite al sistema identificar el idioma correspondiente para la atención. Una vez realizada dicha selección, la plataforma facilita un número de teléfono local, a través del cual la persona informante podrá contactar con personal cualificado que le atenderá en el idioma elegido, garantizando así una comunicación accesible y adecuada a sus necesidades.

Canal Presencial / "Face to Face"

Otra de las vías que la Entidad pone a disposición de sus empleados y aquellos terceros que se relacionan con ésta es el canal presencial / "face to face", cuya finalidad es la de permitir la presentación de comunicaciones verbales mediante una reunión presencial o por videoconferencia. En este caso, y teniendo en cuenta la complejidad que conlleva para la Entidad garantizar el anonimato del informante en aquellos casos que así se solicite, la Entidad ha encomendado esta función al experto externo BONET consulting, el cual se encarga de recibir y gestionar las comunicaciones con estas características, así como aquellas otras en las que se identifiquen los informantes y se requiera la gestión presencial. En este sentido, el experto externo garantiza la protección de la identidad del informante tanto en el proceso de solicitud de cita previa, en la presentación de una comunicación en formato presencial, como en el lugar de realización de la misma.

A efectos de garantizar la seguridad y preservar la integridad de la información que aporte el informante, la reunión será grabada conforme a lo estipulado en la Ley y con el consentimiento previo del informante. Dicha reunión quedará documentada en un formato seguro, con las medidas de seguridad y anonimización requeridas por el marco normativo. En esta línea, **BONET consulting** dispone y habilitará los mecanismos tecnológicos necesarios para el envío de documentación complementaria a la información aportada en la reunión.

Para poder hacer uso de este canal, la Entidad ha habilitado un teléfono y un correo electrónico de contacto para solicitar la presentación de comunicaciones en este formato, cuya atención y coordinación de la reunión será realizada exclusivamente por BONET consulting. Los datos de contacto para realizar esta solicitud están debidamente publicados en la página web de la Entidad y son los siguientes:

- **Teléfono**:

  El horario de atención al informante es el siguiente:

  - De lunes a jueves de 8:30 a 14:00 y de 15:00 a 18:00 horas.
  - Viernes de 8:30 a 14:30 horas.

- **E-mail**: smithnephew@sistema-interno-informacion.com

Al objeto de garantizar las medidas de protección y seguridad necesarias de este tipo de comunicaciones, no se podrán realizar ni se registrarán comunicaciones presentadas directamente por teléfono o e-mail. Estas dos herramientas están habilitadas exclusivamente para coordinar con el personal técnico día, hora y lugar para realizar la comunicación en formato presencial

Control de Documentos

Document Localisation	
Idioma	Español
Departamentos	OEC & People
País	España

Version Control Record		
Versión	Fecha	*Comentarios*
1.0	29/10/2026	Nuevo documento

Aprobación del documento		
Autora: Katiucia Marques	People Advisory Senior Consultant	DocuSigned by: Katiucia Marques 6ED1B49792FA4F1...
Aprobadora: Sandra Cirera	Compliance Director	Firmado por: Sandra Cirera C00B56B2720E475...

ANEXO I CANALES EXTERNOS DE INFORMACIÓN AUTONÓMICOS

COMUNIDAD AUTÓNOMA	CANAL EXTERNO	VÍA DE ACCESO
Cataluña	Oficina Antifrau de Catalunya (OAC)	https://www.antifrau.cat/es/es
Valencia	Agencia de Prevención y Lucha contra el Fraude y la Corrupción (AVAF)	https://www.antifraucv.es/
Navarra	Oficina de Buenas Prácticas y Anticorrupción (OANA)	https://oana.es/es
Andalucía	Oficina Andaluza contra el Fraude y la Corrupción (OAAF)	https://antifraudeandalucia.es/
Galicia	Autoridad Gallega de Protección de la Persona Informante (AGPI)	https://www.apigalicia.gal/es
Castilla y León	Autoridad Independiente en materia de Corrupción de Castilla y León (AICCyL)	https://www.aiccyl.es/
Castilla La Mancha	Consejo Regional de Transparencia y Buen Gobierno de Castilla-La mancha (CRT CLM)	https://consejotransparenciaclm.es/
Comunidad de Madrid	Consejo de Transparencia y Protección de Datos (CTPD)	https://www.comunidad.madrid/consejo-transparencia