



Until we are all equal

FUNDACIÓN PLAN INTERNATIONAL ESPAÑA

**PROTOCOLO
DE GESTIÓN DE SISTEMA INTERNO DE INFORMACIÓN**

V.00

En Madrid, a 26 de Febrero de 2026

La edición de este documento corresponde únicamente al Responsable del Tratamiento, por lo cual, cualquier otra persona o entidad que acceda al presente, lo hará al sólo efecto informativo. Si tiene dudas respecto de si la versión publicada es la actual, podrá comunicarse con el Responsable del Tratamiento a través de los canales indicados en el presente documento. El mismo se considera, tras su impresión, una COPIA NO CONTROLADA, por lo que una vez impreso no se garantiza la vigencia del presente documento.

ÍNDICE

1. OBJETIVO, ALCANCE, Y USUARIOS	3
2. PRINCIPIOS INSPIRADORES DEL SISTEMA	3
3. TRANSPARENCIA DE LA INFORMACIÓN	3
4. CANAL HABILITADO PARA LA REMISIÓN DE DENUNCIAS	4
5. ÁMBITO MATERIAL DE APLICACIÓN	4
6. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN Y EQUIPO DE GESTIÓN....	6
7. CONFLICTOS DE INTERÉS.....	8
8. PROTECCIÓN DEL INFORMANTE Y DE LAS PERSONAS AFECTADAS. PROHIBIÓN DE REPRESALIAS.....	8
9. PROCEDIMIENTO DE GESTIÓN	10
9.1. Acceso al sistema por parte de los informantes.....	10
9.2. Tramitación de la denuncia.....	12
9.3. Gestión de la información	12
9.4. Análisis, investigación y resolución.....	13
10. LIMITACIÓN DE ACCESO A LOS DATOS	13
11. CRITERIOS DE CONSERVACIÓN DE LOS DATOS PERSONALES	14
12. INCIDENTES DE SEGURIDAD.....	14
13. DERECHOS DE LOS INTERESADOS.....	14
14. PUBLICACIÓN	15
15. HISTORIAL DE CAMBIOS	15

1. OBJETIVO, ALCANCE, Y USUARIOS

El objetivo del presente protocolo es regular y establecer de forma detallada el procedimiento de gestión del Sistema de canal de denuncias implantado en la entidad, de conformidad con lo establecido por la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, así como por la normativa vigente en protección de datos, esto es, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (en adelante, RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

El presente documento resulta de aplicación, tanto a las personas trabajadoras autorizadas a gestionar las denuncias interpuestas por los informantes, como a aquellos encargados del tratamiento de la organización, quedando todos ellos sujetos a lo establecido en el presente protocolo, debiendo actuar en todo momento siguiendo las instrucciones aquí establecidas.

2. PRINCIPIOS INSPIRADORES DEL SISTEMA

Se exponen, a continuación los principios inspiradores del Sistema de información implantado en la organización:

- Principios de independencia y autonomía en la recepción y tratamiento de la información.
- Principio de accesibilidad.
- Principio de confidencialidad y de protección de datos personales.
- Principio de defensa del informante.
- Principio de presunción de inocencia y al honor de las personas afectadas.
- Principio de publicidad del sistema en el seno de la organización.

3. TRANSPARENCIA DE LA INFORMACIÓN

La organización tiene establecidos los medios a través de los cuales se debe facilitar al interesado la información estipulada en los artículos 13 y 14 del RGPD y 11 de la LOPDGDD. La información básica a la que se refiere el apartado anterior deberá contener, al menos:

- a) La identidad del responsable del tratamiento y de su representante, en su caso.
- b) La finalidad del tratamiento.
- c) Posibilidad y medio para solicitar más información y ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

La información facilitada al interesado deberá constar de forma concisa, transparente, inteligible, de fácil acceso y con un lenguaje claro y sencillo, identificando en todo momento a la organización.

Asimismo, la entidad ha implementado en el Canal medios destinados a facilitar a los informantes toda la información exigida por la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

4. CANAL HABILITADO PARA LA REMISIÓN DE DENUNCIAS

Mediante la presente, se informa al personal correspondiente acerca del procedimiento establecido para atender las comunicaciones de los interesados, definiendo de forma clara los mecanismos a través de los cuales podrá efectuarse las correspondientes denuncias por parte de los informantes.

A los efectos descritos, la organización ha habilitado un Sistema interno de información, el cual se encuentra alojado en la siguiente **URL/QR**:



Para garantizar la contestación en plazo a las solicitudes recibidas, el buzón habilitado debe ser diariamente examinado por la persona designada a tal fin. A estos efectos, debe tenerse en cuenta que, **a pesar de que los informantes remitan su comunicación a través de canales no habilitados o a miembros del personal no responsable del tratamiento, el artículo 9.2.g) de la Ley 2/2023 establece que el receptor de la comunicación deberá remitirla inmediatamente al Responsable del Sistema**, bajo advertencia de su obligación de confidencialidad y de la tipificación como infracción muy grave de su quebranto, debiendo proveer de los detalles, copias de la comunicación, documentación y cualquier otro dato que al respecto se posea.

5. ÁMBITO MATERIAL DE APLICACIÓN

Se expone, a continuación, el ámbito material de aplicación de los Sistemas internos de información a partir de lo dispuesto, tanto en 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, como 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. Sin perjuicio de lo anterior, es importante destacar que la lista de lo que se puede denunciar a través de un canal de denuncias puede variar dependiendo del sector y la organización en particular:

a) Acciones u omisiones que pudieran constituir infracciones relativas a los siguientes ámbitos de aplicación:

- 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;

b) infracciones que afecten a los intereses financieros de la Unión tal como se contemplan en el artículo 325 del TFUE;

c) infracciones relativas al mercado interior, tal 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 del impuesto sobre sociedades.

d) Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave, incluyéndose todas aquellas infracciones penales o administrativas graves o muy graves que impliquen un quebranto económico para la Hacienda Pública y para la Seguridad Social.

e) Conflictos laborales así como infracciones del Derecho laboral, incluyéndose las relativas en materia de seguridad y salud en el trabajo.

f) Violaciones de códigos éticos, políticas y procedimientos internos de la empresa, incluyendo prácticas comerciales poco éticas o incumplimiento de regulaciones, uso de información privilegiada o aprovechamiento de la posición de la empresa para beneficio personal.

Por su parte, el Sistema interno de información no se encuentra destinado a los siguientes supuestos:

1.- Quejas o reclamaciones de clientes o proveedores. Estas situaciones deben ser tratadas a través de los canales habituales de atención al cliente o proveedor.

2.- Conflictos entre empleados. Las disputas entre empleados deben ser resueltas mediante los procedimientos internos de la empresa, como los mecanismos de mediación o arbitraje.

3.- Asuntos personales no relacionados con la empresa. Los asuntos personales de los empleados que no estén relacionados con la empresa no deben ser tratados a través del canal de denuncias.

4.- Situaciones que no impliquen incumplimiento de normativas, Códigos éticos o políticas. El canal de denuncias debe ser utilizado exclusivamente para reportar conductas contrarias a la ley o las políticas internas de la empresa.

6. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN Y EQUIPO DE GESTIÓN

Para garantizar una coordinación eficaz de las denuncias recibidas, el órgano de gobierno es el competente para designar y destituir al Responsable del Sistema interno de información. Dicha designación puede realizarse, tanto a una persona concreta, como a un órgano colegiado, conformado por un mínimo de tres personas. En caso de designar a un órgano colegiado, el Responsable del sistema deberá delegar en uno de sus miembros las facultades de gestión del Sistema interno de información y de tramitación de expedientes de investigación. Asimismo, dicha gestión puede ser encomendada a un tercero externo, ya sea persona física o jurídica, siempre ofrezca garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones. Este tercero externo tendrá la consideración de encargado del tratamiento a efectos de la legislación sobre protección de datos personales, por lo que resultará preceptivo suscribir el correspondiente contrato de procesamiento de datos a la luz de lo dispuesto por el artículo 28 RGPD.

Tanto el nombramiento como el cese de la persona física individualmente designada, así como de las integrantes del órgano colegiado, deberán ser notificados a la Autoridad Independiente de Protección del Informante, A.A.I., o, en su caso, a las autoridades u órganos competentes de las comunidades autónomas en el ámbito de sus respectivas competencias, en el plazo de los **diez días hábiles siguientes**, especificando, en el caso de su cese, las razones que han justificado el mismo.

El Responsable del Sistema deberá desarrollar sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad 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 Responsable del Sistema -persona física o la entidad en quien el órgano colegiado responsable haya delegado sus funciones-, será un directivo de la entidad, que ejercerá su cargo con independencia del órgano de administración o de gobierno de la misma. Cuando la naturaleza o la dimensión de las actividades de la entidad no justifiquen o permitan la existencia de un directivo Responsable del Sistema, será posible el desempeño ordinario de las funciones del puesto o cargo con las de Responsable del Sistema, tratando en todo caso de evitar posibles situaciones de conflicto de interés.

En el supuesto de que ya existiera una persona responsable de la función de cumplimiento normativo o de políticas de integridad, cualquiera que fuese su denominación, podrá ser esta la persona designada como Responsable del Sistema, siempre que cumpla los requisitos antedichos.

Así pues, la organización ha designado al siguiente órgano colegiado como Responsable del Sistema:

INTEGRANTES:

Belen Kindelan con cargo Gerente RRHH, número de teléfono **649 98 13 41** y correo electrónico Belen.Kindelan@plan-international.org

Fernando Álvarez con cargo Director de Marketing, número de teléfono **608832461** y correo electrónico Fernando.Alvarez@plan-international.org

RESPONSABLE SUSTITUTO

Carlos Mayo con cargo Gerente de RRHH, y correo electrónico Carlos.mayo@plan-international.org

RESPONSABLE DE LA GESTIÓN Y TRAMITACIÓN DE EXPEDIENTES:

Fernando Álvarez con cargo Director de Marketing, número de teléfono **608832461** y correo electrónico Fernando.Alvarez@plan-international.org

Así pues, la organización ha designado para la gestión del Sistema, al siguiente tercero externo:

GESTOR EXTERNO: FORLOPD | SEGURIDAD Y PRIVACIDAD DE DATOS, S.L con teléfono de contacto [963 122 868](tel:963122868) y correo electrónico canaldenuncias@forlopd.es

PERSONA DE CONTACTO DE LA ORGANIZACIÓN: Carlos Mayo con cargo Gerente de RRHH, y correo electrónico Carlos.mayo@plan-international.org

7. CONFLICTOS DE INTERÉS

La presentación de una comunicación que afecte directamente a personas que puedan participar activamente en la gestión e investigación de la misma, serán excluidos de forma automática durante todo el proceso de investigación y análisis hasta su resolución, con el fin de evitar cualquier tipo de conflicto de interés e incompatibilidad, y garantizar así la objetividad e independencia de las actuaciones realizadas.

Los miembros excluidos del proceso de gestión y seguimiento de la comunicación estarán obligados a mantener la máxima confidencialidad, quedando prohibido el acceso directo o indirecto a cualquier tipo de información que pudiera revelar la identidad del denunciante, así como del proceso de investigación en curso.

8. PROTECCIÓN DEL INFORMANTE Y DE LAS PERSONAS AFECTADAS. PROHIBIÓN DE REPRESALIAS

La Ley 2/2023, de 20 de febrero, tiene como objetivo establecer un marco normativo para proteger a las personas que informen sobre infracciones normativas y de lucha contra la corrupción, garantizando que puedan hacerlo de forma segura y sin temor a represalias.

A título enunciativo puede ser constitutivo de represalia:

- La suspensión del contrato de trabajo, despido o extinción de la relación laboral, por cualquier motivo o modificación sustancial de las condiciones de trabajo, falta de conversiones contractuales, etc.
- Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.

- Evaluación o referencias negativas respecto al desempeño laboral o profesional.
- Inclusión en listas negras o difusión de información que dificulten o impidan el acceso al empleo o la contratación de obras o servicios.
- Denegación o anulación de una licencia o permiso.
- Denegación de formación.
- Discriminación, o trato desfavorable o injusto.

A tales fines, se establece la obligación de adoptar medidas que garanticen la protección de informante, asegurando, en todo momento, su integridad física y psicológica, evitando, asimismo, cualquier tipo de represalia o discriminación.

Condiciones de protección:

Las personas que comuniquen o revelen infracciones tendrán derecho a protección siempre que concurren 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 esta ley,
- b. la comunicación o revelación se haya realizado conforme a los requerimientos previstos 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.

Quedan expresamente excluidos de la protección prevista aquellas personas que comuniquen o revelen:

- a. Informaciones contenidas en comunicaciones que hayan sido inadmitidas por alguna de las causas previstas.
- 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.

Las personas que hayan realizado la comunicación de forma anónima pero posteriormente sean identificadas tendrán derecho a la protección, siempre que se cumplan las condiciones anteriormente previstas.

Estas medidas de protección también se aplicarán, en su caso, a:

- a. Personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso,
- b. Personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante, y
- c. personas jurídicas, para las que trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa. A estos efectos, se entiende que la participación en el capital o en los derechos de voto correspondientes a acciones o participaciones es significativa cuando, por su proporción, permite a la persona que la posea tener capacidad de influencia en la persona jurídica participada.

Asimismo, las personas afectadas por la comunicación tendrán derecho a:

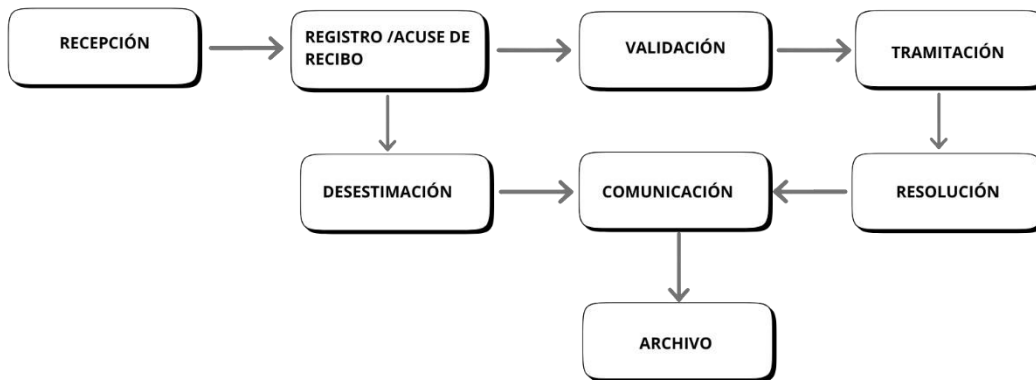
- presunción de inocencia;
- derecho de defensa y al derecho de acceso al expediente en los términos regulados en la ley;
- confidencialidad de la identidad, de los hechos y de los datos del procedimiento.

9. PROCEDIMIENTO DE GESTIÓN

9.1. Acceso al sistema por parte de los informantes

El Canal establecido permite realizar las comunicaciones de forma escrita o verbal. Al hacer la comunicación, en caso de que informante se identifique, podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las correspondientes notificaciones de seguimiento. En caso de que el interesado realice la comunicación de forma anónima, se le asignará una URL para que pueda realizar el correspondiente seguimiento de la denuncia.

Así pues, los informantes, sean anónimos o no, accediendo a la plataforma del Sistema podrá comprobar los siguientes estados en los que se encuentra la denuncia en cada una de las distintas fases del procedimiento de tramitación:



Consiguientemente, debe tenerse en cuenta que, a solicitud del informante, la comunicación de la denuncia también podrá realizarse de forma presencial, a través de reunión presencial, telefónicamente o mediante sistema de mensajería de voz, dentro del plazo de siete días desde que se efectúe la solicitud. En este último caso, la comunicación será grabada, debiendo informar al interesado de este aspecto antes del inicio de la reunión. Asimismo, se deberá proporcionar la información sobre protección de datos especificada en el apartado «3. Transparencia de la información», del presente documento.

La información remitida por la persona informante podrá ser comunicada consignando sus datos a través del correspondiente formulario o de forma anónima. A estos efectos, la organización ha establecido mecanismos para preservar la identidad del informante anónimo. No obstante, en todo caso, la identidad de los interesados (anónimos o no) será en todo caso reservada, por lo que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros, con las siguientes excepciones:

- ▶ Autoridad judicial, Ministerio Fiscal o a la autoridad administrativa competente, en el marco de una investigación penal, disciplinaria o sancionadora.

En este supuesto, antes de revelar su identidad se comunicará a la persona informante sobre dicho extremo, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial.

Sin perjuicio de los derechos que le corresponden de acuerdo a la normativa sobre protección de datos, el sistema ofrece al informante la posibilidad de aportar todos los datos y documentos relacionados con los hechos denunciados, así como la oportunidad de comprobar, rectificar la transcripción del mensaje.

9.2. Tramitación de la denuncia

La comunicación de la denuncia por parte de los interesados se efectuará a través del Canal habilitado en el portal web, cumplimentando el modelo de formulario que encontrará al acceder al Sistema. Dicha comunicación deberá contener, al menos, la siguiente información:

- a. Datos del denunciante (en caso de no seleccionar la opción de denuncia anónima).
- b. Relación con la entidad.
- c. Relación de los hechos.
- d. Personas implicadas y posibles testigos.
- e. En su caso, documentación que pueda facilitar la investigación de la denuncia
- f. Canal de comunicación (en caso de comunicación anónima el sistema le proveerá de una URL a la cual puede acceder para hacer seguimiento de su denuncia).

Sin perjuicio de lo antedicho, debe tenerse en cuenta lo establecido respecto a la recepción de las denuncias por canales no habilitados o a personal no designado en el apartado «4. *Canal habilitado para la remisión de denuncias*».

9.3. Gestión de la información

Recibida la denuncia del informante en el Sistema de Gestión de Información, el software asignará a la misma un número de referencia registrando la fecha de recepción, así como las actuaciones desarrolladas sobre dicha información y, en su caso, las conversaciones mantenidas con el informante, testigos y personas afectadas, las medidas adoptadas y la fecha de cierre.

Recogida la información, el personal designado deberá acusar de recibo al informante en un plazo no superior a **siete días naturales** siguientes a su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación. En caso de que la denuncia se realice de forma anónima, se dejará constancia en el Sistema, debiendo el interesado acceder con la URL asignada para conocer el estado de la denuncia realizada.

9.4. Análisis, investigación y resolución

Recibida la comunicación, el personal designado para su gestión procederá al análisis de la información a efectos de valorar su procedencia, dando archivo a aquellas conductas que no estén incluidas en el ámbito de aplicación de la Ley 2/2023.

En caso de ser admitida a trámite, se procederá a realizar las oportunas investigaciones a fin de esclarecer los hechos presentados. Con esta finalidad, el órgano gestor podrá solicitar información adicional a la persona informante, así como entrevistar a aquellas personas que se considere de relevancia, incluyendo a las personas afectadas.

Una vez concluida la fase de investigación, se realizará un informe de conclusiones remitiéndose el mismo, tanto al órgano de dirección como al informante.

El plazo máximo para dar respuesta a las actuaciones de investigación **no será superior a tres meses** a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo, a tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, este podrá extenderse hasta un máximo de otros tres meses adicionales.

Una vez realizado este trámite se determinará, en su caso, las sanciones o medidas disciplinarias adecuadas a cada supuesto. En caso de que el hecho comunicado pudiera ser constitutivo de delito, deberá elevarse a las autoridades competentes.

10. LIMITACIÓN DE ACCESO A LOS DATOS

De conformidad con lo establecido por el artículo 32 de la Ley 2/2023, el acceso a los datos personales contenidos en el Sistema interno de información se encuentra limitado, exclusivamente a las figuras, que a continuación se expresan, y siempre dentro del ámbito de sus competencias y funciones:

- a) El Responsable del Sistema y a quien lo gestione directamente.
- b) El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder a la adopción de medidas disciplinarias contra un trabajador. En el caso de los empleados públicos, el órgano competente para la tramitación del mismo.
- c) El responsable de los servicios jurídicos de la entidad u organismo, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.
- d) Los encargados del tratamiento que eventualmente se designen.
- e) El delegado de protección de datos.

Sin perjuicio de lo anterior y de conformidad con la normativa aplicable, será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

11. CRITERIOS DE CONSERVACIÓN DE LOS DATOS PERSONALES

Los datos que sean objeto de tratamiento se conservarán en el Sistema únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.

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

En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, se procederá a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema. No obstante, se señala que en cumplimiento de lo dispuesto por el artículo 26 de la Ley 2/2023, en ningún caso, los datos podrán conservarse los datos por un período superior a diez años.

12. INCIDENTES DE SEGURIDAD

Todos los usuarios sujetos al presente protocolo tienen el deber de notificar al Responsable de tratamiento sobre el conocimiento o la sospecha razonable de una violación de seguridad de los cuales sean objeto los datos personales, mediante correo electrónico dirigido a la dirección dpo_spno@plan-international.org sin dilación indebida y, en cualquier caso, dentro de las 24 horas a partir del conocimiento o la sospecha razonable, especificando la naturaleza del incidente, la categoría y número de afectados, las posibles consecuencias sobre los mismos y las medidas tomadas o propuestas para abordar la situación. Si no es posible facilitar la información simultáneamente, deberá facilitarse de manera gradual sin dilación indebida.

13. DERECHOS DE LOS INTERESADOS

Los interesados podrán solicitar más información acerca del tratamiento de sus datos personales así como ejercer en cualquier momento y, de forma gratuita, los derechos de acceso, rectificación y supresión, así como solicitar que se limite el tratamiento de sus datos personales, oponerse al mismo, solicitar la portabilidad de estos (siempre que sea técnicamente posible) o retirar el consentimiento prestado y, en su caso, a no ser objeto de una decisión basada únicamente en un tratamiento automatizado, incluido la elaboración de perfiles.

Para ello podrá emplear, en su caso, los formularios habilitados por la organización, o bien dirigir un escrito a través de los siguientes canales:

CORREO POSTAL DE LA ORGANIZACIÓN: Calle Pantoja 10, 28002, Madrid.

E-MAIL DE LA ORGANIZACIÓN: dpo_spno@plan-international.org

A los efectos oportunos, le informamos que se le podrá solicitar su DNI o cualquier otro documento análogo, con la finalidad de acreditar su identidad, siempre que ello no pueda realizarse por otros medios menos intrusivos.

14. PUBLICACIÓN

El presente protocolo debe ser conocido y estar accesible para el órgano directivo de la organización todos los integrantes de la entidad que en el ejercicio de sus funciones laborales tienen atribuidas las competencias relacionadas con la recepción, registro, tramitación de las comunicaciones efectuadas a través del Sistema interno de información implantado en la Organización.

Igualmente, se pone en conocimiento de los Encargados del Tratamiento, que en virtud del contrato de encargo de tratamiento han asumido la obligación de prestar apoyo a la Organización en la gestión de la tramitación, o en su caso, hayan sido autorizados a la gestión de las comunicaciones.

15. HISTORIAL DE CAMBIOS

Versión	Fecha	Descripción del cambio
V.00	26/02/2026	Primer ejemplar