



**POLÍTICA DEL SISTEMA
INTERNO DE INFORMACIÓN**

Índice

1. CONTROL DE VERSIONES	4
2. OBJETO	6
3. COMPROMISO DE LA ORGANIZACIÓN	6
4. ÁMBITO DE APROBACIÓN, APLICACIÓN Y ACTUALIZACIONES	7
4.1. Aprobación	7
4.2. Aplicación	7
4.3. Actualizaciones	8
5. ALCANCE	8
6. DEFINICIONES	9
7. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN DE DOVALUE	10
8. SISTEMA INTERNO DE INFORMACIÓN DE DOVALUE Y CANALES EXTERNOS DE INFORMACIÓN	12
8.1. SISTEMA INTERNO DE INFORMACIÓN DE DOVALUE.	12
8.1.1. OBJETO DEL SISTEMA INTERNO DE INFORMACIÓN.	12
8.1.2. ACCESO Y FUNCIONAMIENTO DEL SISTEMA INTERNO DE INFORMACIÓN.	13
8.2. CANALES EXTERNOS DE INFORMACIÓN.	14
9. PRINCIPIOS DEL SISTEMA INTERNO DE INFORMACIÓN	15
10. PARÁMETROS DE PROTECCIÓN	17
10.1. PERSONAS SUSCEPTIBLES DE PROTECCIÓN	17
10.2. CONDICIONES DE LA PROTECCIÓN	18
10.3. MEDIDAS DE PROTECCIÓN AL INFORMANTE Y TERCEROS RELACIONADOS	18
10.4. MEDIDAS DE PROTECCIÓN A LAS PERSONAS AFECTADAS POR LA COMUNICACIÓN	20
10.5. CUMPLIMIENTO DE PLAZOS	21
10.6. ACTIVACIÓN DE LA PROTECCIÓN	22
11. CONSECUENCIAS DEL INCUMPLIMIENTO	22
12. FORMACIÓN	23

13. PUBLICIDAD	24
ANEXOS	25
ANEXO 1. Plantilla Modelo de Formulación de Comunicación	25
ANEXO 2. Listado ejemplificativo de conductas consideradas represalias.	26

1. CONTROL DE VERSIONES

CONTROL DE VERSIONES	
Compañía	doValue Spain Servicing, S.A.U. y sus filiales
Título	Política del Sistema Interno de Información
Versión	V.3.0
Documento	Política 6
Elaborado por	Compliance Officer
Fecha Aprobación	31/07/2026
Responsable de la aprobación	Consejo de administración doValue Spain
Fecha ratificación	09/2026
Responsable ratificación	n/a
Política o normas modificadas / derogadas	Política del Sistema Interno de Información v.2
Modificaciones de la versión	Se actualizan diferentes apartados para adaptarlos a las recomendaciones de la AIPI y algunos matices de la Ley 2/2023. Adicionalmente, se incorporan los plazos principales previstos en la Ley 2/2023.
Fecha última actualización	31/07/2026

Versión	Causa del Cambio	Responsable	Fecha aprobación	Fecha ratificación
1.0	Versión Inicial	Cumplimiento Normativo	16/06/2023	16/06/2023
2.0	Versión 2: - Modificación del Responsable del Sistema Interno de Información, por un Órgano colegiado que se denominará Comité del Sistema Interno de Información (CSII) y adaptaciones consecuentes. - Se incluye en el punto 4. el objeto del Sistema Interno de Información, el acceso y funcionamiento del sistema interno de información y los canales externos de información. - Se incluye en el punto 5. el principio de prohibición de	Cumplimiento Normativo	16/03/2026	16/03/2026

	represalias frente a Informantes y Terceros relacionados.			
3.0	Se actualizan diferentes apartados para adaptarlos a las recomendaciones de la AIPI y algunos matices de la Ley 2/2023. Adicionalmente, se incorporan los plazos principales previstos en la Ley 2/2023.	Compliance Officer	31/07/2026	09/2026

2. OBJETO

La presente Política tiene por objeto establecer los principios, responsabilidades y normas generales que regulan el funcionamiento del Sistema Interno de Información (en adelante, el "**SII**") de doValue Spain Servicing, S.A.U. (en adelante, conjuntamente, "**doValue**", "**DVSP**", la "**Organización**" o la "**Compañía**") y sus filiales.

El SII constituye el cauce preferente para la comunicación y gestión de informaciones sobre acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea, infracciones penales o administrativas graves o muy graves, incumplimientos del Código de Conducta o de la normativa interna aplicable, así como cualesquiera otras conductas contrarias a los principios éticos y de cumplimiento de la Organización.

Asimismo, la presente Política establece los principios de actuación, las garantías de protección de los informantes y demás personas afectadas, así como las medidas destinadas a asegurar la confidencialidad, independencia, ausencia de represalias y adecuada gestión de las comunicaciones recibidas a través del Sistema Interno de Información.

Esta Política desarrolla los requisitos establecidos 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, y se complementa con el **Procedimiento de Gestión del Sistema Interno de Información**, que regula el funcionamiento operativo del sistema y la tramitación de las comunicaciones recibidas.

3. COMPROMISO DE LA ORGANIZACIÓN

doValue y sus filiales mantienen un firme compromiso con la ética, la integridad, la transparencia y el cumplimiento normativo como principios fundamentales de su modelo de gobierno corporativo y de su cultura organizativa.

En este marco, la Organización promueve un entorno en el que todas las personas puedan comunicar, de buena fe y sin temor a represalias, cualquier conducta, actuación u omisión que pudiera resultar contraria a la legislación aplicable, al Código de Conducta o a la normativa interna de la Organización.

Con el fin de reforzar dichos principios y facilitar la detección temprana de posibles incumplimientos, el Consejo de Administración de doValue Spain Servicing, S.A.U. ha implantado un Sistema Interno de Información y aprobado la presente Política, poniendo a disposición de los grupos de interés canales adecuados para la recepción y gestión de comunicaciones, garantizando en todo momento la confidencialidad, la protección de los informantes, la imparcialidad en la gestión de las investigaciones y el respeto a los derechos de todas las personas involucradas.

Asimismo, la Organización manifiesta su compromiso con la prohibición de cualquier forma de represalia frente a quienes, actuando de buena fe y con motivos razonables, comuniquen o revelen información sobre posibles infracciones, promoviendo una cultura basada en la responsabilidad, la confianza y la mejora continua de los sistemas de control y cumplimiento.

La Organización adoptará las medidas necesarias para garantizar el adecuado funcionamiento del Sistema Interno de Información, la disponibilidad de los recursos necesarios para su gestión efectiva y el cumplimiento de los requisitos establecidos en la normativa aplicable en cada momento.

4. ÁMBITO DE APROBACIÓN, APLICACIÓN Y ACTUALIZACIONES

4.1. Aprobación

La presente Política forma parte del Sistema Interno de Información de doValue y sus filiales, siendo aprobada por los respectivos órganos de administración de las sociedades obligadas a su aplicación, de conformidad con lo previsto 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.

Asimismo, corresponde a los órganos de administración la designación y, en su caso, cese del Responsable del Sistema Interno de Información, así como la supervisión general de su adecuado funcionamiento.

4.2. Aplicación

La presente Política es de obligado cumplimiento para doValue y sus filiales, así como para todos los integrantes de la Organización, incluidos los miembros de los órganos de administración, directivos, empleados, trabajadores cedidos, becarios, personal en formación y cualquier otra

persona que desarrolle su actividad profesional bajo la dirección, supervisión o control de la Organización.

Asimismo, la Organización promoverá el conocimiento y observancia de los principios contenidos en esta Política por parte de proveedores, contratistas, colaboradores externos, socios de negocio y cualesquiera terceros con los que mantenga relaciones profesionales o comerciales.

Todas las personas sujetas a esta Política deberán cumplir su contenido con independencia del cargo, función, modalidad de vinculación o ubicación geográfica desde la que desarrollen su actividad.

4.3. Actualizaciones

La presente Política será objeto de revisión periódica con el fin de garantizar su adecuación a la normativa aplicable, a la estructura organizativa de la Organización, a las recomendaciones de las autoridades competentes y a las necesidades derivadas del funcionamiento efectivo del Sistema Interno de Información.

Las modificaciones de carácter sustancial deberán ser aprobadas por el órgano de administración competente. Las modificaciones de carácter meramente organizativo, operativo o documental que no alteren los principios esenciales de la presente Política podrán ser propuestas por el Comité del Sistema Interno de Información (CSII) para su correspondiente aprobación por el Compliance Officer.

5. ALCANCE

La presente Política tiene por finalidad establecer los principios, garantías y normas de funcionamiento del Sistema Interno de Información de doValue y sus filiales, así como regular la protección de las personas que comuniquen o revelen públicamente información sobre infracciones en los términos previstos en la Ley 2/2023.

Las medidas de protección previstas en esta Política resultarán aplicables, según corresponda, a:

- Los Informantes.
- Los Terceros relacionados.
- Los representantes legales de las personas trabajadoras cuando actúen en funciones de asesoramiento y apoyo al Informante.
- Las Personas afectadas por la Comunicación.

A los efectos de la presente Política, tendrán la consideración de Informantes, Terceros relacionados y Personas afectadas por la Comunicación quienes reúnan los requisitos y condiciones previstos en la Ley 2/2023 y en los apartados siguientes de esta Política.

6. DEFINICIONES

A efectos de la presente Política, serán de aplicación las siguientes definiciones:

- **Comunicación:** Información presentada a través del Sistema Interno de Información relativa a hechos, conductas u omisiones que puedan constituir infracciones comprendidas dentro del ámbito de aplicación de la presente Política.
- **Sistema Interno de Información (SII):** Conjunto integrado de principios, procedimientos, recursos, personas y canales habilitados por la Organización para la recepción, gestión, investigación y seguimiento de las comunicaciones realizadas en el marco de la presente Política.
- **Informante:** Persona física que comunique o revele públicamente información sobre infracciones obtenida en un contexto laboral o profesional y que reúna las condiciones previstas en la Ley 2/2023. Tendrán la consideración de informantes, entre otros, los empleados, trabajadores autónomos, accionistas, miembros del órgano de administración, dirección o supervisión, personas que trabajen para o bajo la supervisión de socios de negocio, voluntarios, becarios, personas en formación y aquellas cuya relación laboral o profesional haya finalizado o no haya comenzado todavía.
- **Persona afectada por la Comunicación:** Persona física o jurídica a la que se atribuyen los hechos, conductas u omisiones descritos en una comunicación recibida a través del Sistema Interno de Información.
- **Terceros relacionados:** Personas físicas o jurídicas vinculadas al Informante que puedan sufrir represalias en un contexto laboral o profesional como consecuencia de una comunicación, incluyendo, entre otros, compañeros de trabajo, familiares, representantes legales de los trabajadores o entidades con las que el Informante mantenga una relación profesional significativa.
- **Responsable del Sistema Interno de Información:** Órgano responsable de la supervisión y funcionamiento del Sistema Interno de Información, designado por el Consejo de Administración de conformidad con la Ley 2/2023. En doValue, dicha función corresponde al Comité del Sistema Interno de Información (CSII).

- **Comité del Sistema Interno de Información (CSII):** Órgano colegiado designado como Responsable del Sistema Interno de Información, responsable de supervisar el adecuado funcionamiento del Sistema, garantizar el cumplimiento de la presente Política y adoptar las decisiones que resulten necesarias para su correcta aplicación.
- **Persona Delegada del Sistema:** Miembro del CSII designado para ejercer las funciones de gestión ordinaria del Sistema Interno de Información, incluyendo la recepción y tramitación de comunicaciones, coordinación de investigaciones, mantenimiento de los registros correspondientes y ejecución de las actuaciones que le encomiende el CSII.
- **Revelación pública:** Puesta a disposición del público de información sobre infracciones en los términos y condiciones previstos en la Ley 2/2023.
- **Represalia:** Cualquier acto u omisión, amenaza o tentativa, prohibido por la normativa aplicable, que provoque o pueda provocar un perjuicio injustificado a una persona como consecuencia de haber realizado una comunicación o revelación pública protegida.
- **Conflicto de interés:** Situación en la que los intereses personales, profesionales o económicos de una persona puedan comprometer o aparentar comprometer su imparcialidad, independencia u objetividad en la gestión o resolución de una comunicación.
- **Buena fe y motivos razonables:** A efectos de esta Política, se entenderá que una comunicación se realiza de forma legítima cuando el informante tenga motivos razonables para considerar que la información comunicada es veraz en el momento de su presentación, con independencia de que posteriormente los hechos puedan resultar acreditados o no.

7. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN DE DOVALUE

La designación de un Responsable del Sistema responde a la obligación establecida en el artículo 8 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.

El Consejo de Administración de doValue Spain Servicing, S.A.U. ha designado como Responsable del Sistema interno de información al **Comité del Sistema Interno de Información (CSII)**, órgano colegiado que actúa

con autonomía e independencia en el ejercicio de sus funciones y que dispone de la competencia, integridad, autoridad y recursos necesarios para garantizar el adecuado funcionamiento del Sistema Interno de Información.

El CSII es el órgano responsable de la supervisión general del Sistema Interno de Información, del seguimiento de su funcionamiento y de la adopción de las decisiones que resulten necesarias para garantizar el cumplimiento de la presente Política y de la normativa aplicable.

La composición del CSII será la siguiente:

- Director de Asesoría Jurídica y Delegado de Protección de Datos
- Directora de Control & ERM y Compliance Officer
- Coordinadora de Control de Reclamaciones
- Director de Relaciones Laborales
- Especialista Senior de Seguridad y Salud

Con el fin de facilitar la gestión ordinaria del Sistema Interno de Información, el CSII designará de entre sus miembros a una persona delegada, a la que corresponderá la gestión operativa del sistema, la recepción y tramitación de las comunicaciones, la coordinación de las actuaciones de investigación y aquellas otras funciones que le sean expresamente encomendadas por el Comité, sin perjuicio de las competencias y responsabilidades que correspondan al propio CSII como Responsable del Sistema.

Cuando concurra una situación de conflicto de interés, ausencia, vacante o cualquier otra circunstancia que pudiera comprometer la independencia o imparcialidad de alguno de sus miembros, éste deberá abstenerse de intervenir en la gestión o toma de decisiones relacionadas con la comunicación afectada, correspondiendo al resto de integrantes del Comité adoptar las medidas necesarias para garantizar la adecuada tramitación del expediente.

El nombramiento, cese y cualquier modificación en la composición del CSII o en la persona en quien se deleguen las facultades de gestión del Sistema serán comunicados a la Autoridad Independiente de Protección del Informante, A.A.I., en los términos y plazos establecidos en la normativa aplicable.

8. SISTEMA INTERNO DE INFORMACIÓN DE DOVALUE Y CANALES EXTERNOS DE INFORMACIÓN

8.1. SISTEMA INTERNO DE INFORMACIÓN DE DOVALUE.

8.1.1. OBJETO DEL SISTEMA INTERNO DE INFORMACIÓN.

doValue dispone de un Sistema interno de información integrado por diferentes canales habilitados para la recepción y gestión de comunicaciones relativas a hechos o conductas conocidos en un contexto laboral o profesional

- A través del Sistema Interno de Información podrán comunicarse, entre otras, las siguientes conductas: Infracciones del Derecho de la Unión Europea comprendidas en el ámbito de aplicación de la Directiva (UE) 2019/1937 y de la Ley 2/2023, de 20 de febrero
- Infracciones penales o administrativas graves o muy graves.
- Infracciones del Código de Conducta de la Organización.
- Incumplimientos de la normativa interna, procedimientos, políticas corporativas o cualesquiera otras conductas irregulares, fraudulentas o contrarias a los principios éticos y de cumplimiento de la Organización.

El Sistema Interno de Información constituye el cauce preferente para la comunicación de este tipo de conductas y tiene por finalidad facilitar su detección temprana, evaluación, investigación y, en su caso, la adopción de las medidas correctoras o disciplinarias que resulten procedentes.

Sin perjuicio de lo anterior, no todas las comunicaciones recibidas a través del Sistema Interno de Información quedarán comprendidas dentro del ámbito de protección previsto por la Ley 2/2023. En particular, las comunicaciones relativas exclusivamente a incumplimientos del Código de Conducta o de la normativa interna que no constituyan infracciones del Derecho de la Unión Europea ni infracciones penales o administrativas graves o muy graves serán gestionadas a través del Sistema, pero no generarán automáticamente las medidas de protección específicamente previstas en la citada Ley.

No obstante, la Organización garantizará en todos los casos la confidencialidad de la información recibida, la protección de los datos personales tratados y una gestión diligente e imparcial de las comunicaciones,

de conformidad con lo previsto en la presente Política y en la normativa aplicable.

La clasificación de una comunicación dentro o fuera del ámbito de protección de la Ley 2/2023 corresponderá al Comité del Sistema Interno de Información o a la persona en quien éste delegue la gestión del Sistema, de acuerdo con el procedimiento interno aplicable.

8.1.2. ACCESO Y FUNCIONAMIENTO DEL SISTEMA INTERNO DE INFORMACIÓN.

La Organización dispone de un Sistema Interno de Información integrado por distintos canales habilitados para la recepción y gestión de comunicaciones relativas a hechos o conductas producidos en un contexto laboral o profesional.

Las comunicaciones podrán presentarse de forma nominativa o anónima, garantizándose en todo caso la confidencialidad de la identidad del informante, de las personas afectadas por la comunicación y de cualquier tercero relacionado, así como la protección de los datos personales tratados.

Las comunicaciones podrán realizarse por escrito, verbalmente o mediante solicitud de reunión presencial, de conformidad con lo previsto en la presente Política y en el Procedimiento de Gestión del Sistema Interno de Información.

Los canales habilitados por la Organización para la presentación de comunicaciones son los siguientes:

- **doValue:** www.dovalue.whistlelink.com
- **TEAM4:** <https://team4.canalhelas.com/home>

Cuando la comunicación se presente a través de las plataformas habilitadas al efecto, el sistema podrá generar credenciales o mecanismos de seguimiento que permitirán al informante consultar el estado de la comunicación y atender las solicitudes de información que le sean dirigidas.

Para los supuestos relacionados con situaciones de acoso laboral, acoso sexual o ciberacoso, la Organización dispone de canales específicos gestionados de conformidad con lo previsto en el Protocolo de Prevención del

Acoso Laboral, Acoso Sexual y Ciberacoso. Estos canales forman parte del marco general de control de la Organización y se gestionarán conforme al procedimiento específico aplicable, sin perjuicio de la supervisión general que corresponde al Comité del Sistema Interno de Información (CSII).

Asimismo, el informante podrá solicitar la celebración de una reunión presencial con la persona delegada por el CSII o con cualquier otro miembro designado por éste. La reunión deberá celebrarse dentro del plazo legalmente establecido, esto es, dentro del plazo máximo de siete (7) días desde su solicitud, de conformidad con la Ley 2/2023, y será documentada mediante grabación, previo consentimiento del informante, o mediante transcripción completa y exacta de su contenido, que podrá ser revisada, rectificada y aceptada por el propio informante.

Cuando una comunicación sea recibida por cualquier miembro del CSII o por cualquier otra persona de la Organización distinta de la persona delegada para la gestión del Sistema, deberá remitirse de forma inmediata y confidencial a dicha persona delegada, a fin de garantizar el adecuado seguimiento del procedimiento y la protección de los derechos de los informantes, personas afectadas y terceros relacionados.

Todas las comunicaciones recibidas serán gestionadas de conformidad con lo previsto en el Procedimiento de Gestión del Sistema Interno de Información, garantizando el cumplimiento de las obligaciones de confidencialidad, protección de datos, independencia, objetividad y ausencia de represalias previstas en la normativa aplicable y en la presente Política.

Las comunicaciones podrán recibirse a través de los canales principales del Sistema Interno de Información o mediante otros canales corporativos habilitados específicamente para determinadas materias. En todos los casos, las comunicaciones que entren dentro del ámbito de aplicación de la presente Política serán incorporadas al Sistema Interno de Información y gestionadas conforme al Procedimiento de Gestión del Sistema Interno de Información

8.2. CANALES EXTERNOS DE INFORMACIÓN.

Sin perjuicio de la utilización del Sistema Interno de Información de la Organización, los Informantes podrán comunicar las infracciones

comprendidas dentro del ámbito de aplicación de la Ley 2/2023 directamente ante la Autoridad Independiente de Protección del Informante (A.A.I.) o ante cualesquiera otras autoridades u organismos competentes que resulten aplicables en cada caso.

La Organización pondrá a disposición de los potenciales Informantes información actualizada sobre los canales externos de información habilitados por las autoridades competentes y facilitará su acceso a través de los medios corporativos que resulten oportunos.

Entre otros, podrán utilizarse los siguientes canales:

- Canal externo de la Autoridad Independiente de Protección del Informante (A.A.I.).
<https://www.proteccioninformante.gob.es/canales-de-presentacion-de-informaciones>
- Canales externos habilitados por autoridades autonómicas competentes.
<https://www.proteccioninformante.gob.es/informacion-sobre-otros-canales-externos-de-informacion>
- Canales externos establecidos por organismos, instituciones o autoridades de la Unión Europea cuando resulten aplicables.

La utilización de los canales externos de información no requerirá la utilización previa del Sistema Interno de Información de la Organización.

9. PRINCIPIOS DEL SISTEMA INTERNO DE INFORMACIÓN

La presente Política ha considerado los estándares más avanzados en esta para afirmar su compromiso y voluntad con la aplicación de las máximas garantías de protección para los Informantes, tanto desde el punto de vista de la protección de su identidad como de la ausencia de represalias hacia los mismos.

Por este motivo, en el funcionamiento del Sistema interno de información de la Compañía, se seguirán los siguientes Principios:

- (i) **Principio de Independencia:** se garantiza la autonomía y la evitación de conflictos de interés en el funcionamiento del Sistema interno de

información, así como en las diferentes fases de gestión de la Comunicación recibida, análisis, investigación y resolución de la misma, y, finalmente, en la potencial aplicación de los mecanismos de reacción o *corporate defense*, procurando siempre la protección de dos principios elementales:

- La voluntad de cumplimiento normativo de la Organización.
- El mejor interés corporativo, legítimo de la entidad en contraposición con cualquier otro interés personal, de un grupo o de otro tercero.

(ii) **Principio de Tolerancia Cero y Respeto:** La Compañía ha implementado el Sistema interno de información en base a su compromiso de tolerancia cero con las conductas contrarias a los principios éticos, de cumplimiento y de evitación de delitos que forman parte de su voluntad corporativa de Compliance. Para ello, en todas las comunicaciones y decisiones inherentes al funcionamiento del Sistema interno de información, se respetará y protegerá la figura del informante o *whistleblower*, garantizándose la ausencia de cualquier represalia, consecuencia negativa o conducta perjudicial para el mismo por el mero hecho de la comunicación e interposición de una comunicación.

(iii) **Principio de Confidencialidad:** de acuerdo a lo dispuesto por el artículo 24 de la Ley Orgánica 3/2018 de protección de datos y garantía de los derechos digitales, así como de conformidad con los criterios establecidos en la ley 2/2023, de 20 de febrero.

Con especial énfasis, La Compañía garantiza y vela por la confidencialidad, especialmente referida a cualquier dato que pueda desvelar la identidad de la Persona afectada por la comunicación o, también, al propio contenido de las Comunicaciones.

Estas garantías aplican no sólo a las Comunicaciones en las que el Informante ha optado por su identificación, sino también en aquellas dónde se haya optado por la opción anónima.

(iv) **Buena fe, objetividad y honradez:** recíprocamente a la exigencia de buena fe en la interposición de Comunicaciones, la Organización

procurará alcanzar, a través del análisis e investigación de estas , un conocimiento debido y objetivo de su contenido.

Todo ello, a través del honrado propósito de proteger los bienes jurídicos en juego en las decisiones y actos realizables en el seno de la Organización, así como en el análisis de las comunicaciones que versen sobre la no adecuación de los mismos a los estándares y obligaciones éticas, normativas y de prevención de delitos existentes en la entidad.

(v) Principio de prohibición de represalias / conductas perjudiciales frente a Informantes y Terceros relacionados: doValue y sus filiales prohíben la adopción de represalias contra cualquier Persona Informante o Tercero relacionado, incluyendo las amenazas de represalia y las tentativas de represalia. Esta prohibición abarca, además de las represalias en sentido estricto, cualquier trato adverso o conducta perjudicial relacionada con la comunicación. En el caso de que la Compañía tuviera conocimiento de que se está produciendo o se ha producido una represalia, la Organización adoptará las medidas de protección necesarias para detener, abordar y remediar tal situación.

10. PARÁMETROS DE PROTECCIÓN

10.1. PERSONAS SUSCEPTIBLES DE PROTECCIÓN

La Compañía brindará protección tanto al Informante de buena fe como a los Terceros relacionados frente al eventual perjuicio que estos puedan sufrir por informar sobre posibles infracciones de las que hayan tenido conocimiento, así como a aquellas personas que hayan realizado una revelación pública sobre una de las infracciones que entran dentro del ámbito de aplicación del Sistema interno de información.

Asimismo, la Organización extenderá la protección, en los términos legalmente previstos para este supuesto, a las Personas afectadas por la Comunicación.

No obstante, y según lo dispuesto con anterioridad, las personas que informen sobre infracciones no contempladas en la Ley 2/2023, de 20 de febrero, quedarán fuera del ámbito de protección de la misma.

10.2. CONDICIONES DE LA PROTECCIÓN

Se considera **Informante de buena fe** aquel que tenga motivos razonables para pensar que la información referida es veraz en el momento de la Comunicación, aun cuando no aporten pruebas concluyentes. La protección del Informante no decae por el hecho de que la comunicación finalmente no prospere o los hechos no resulten acreditados, siempre que existieran dichos motivos razonables, y se reconoce con independencia del canal utilizado. Toda persona protegida tendrá derecho a las medidas de apoyo previstas en la Ley 2/2023 (información, asesoramiento y asistencia), sin que se le pueda exigir la renuncia anticipada a estos derechos.

Quedan **expresamente excluidas** del Sistema interno de información de La Compañía las informaciones contenidas en Comunicaciones que hayan sido, previamente, inadmitidas por cualquier otro mecanismo corporativo de comunicación en el que ya, de manera específica, se haya inadmitido, evaluado o resuelto la Comunicación que contiene, precisamente, dichas informaciones, siempre y cuando no se aporten hechos o pruebas adicionales y nuevas.

Del mismo modo, se inadmitirán, también, las informaciones cuyos hechos no se encuentren comprendidos en el ámbito de aplicación del Sistema interno de información de DOVALUE y sus filiales.

10.3. MEDIDAS DE PROTECCIÓN AL INFORMANTE Y TERCEROS RELACIONADOS

La Compañía son responsables de garantizar la protección a los Informantes y Terceros relacionados, de conformidad con el artículo 39 de la Ley 2/2023, de 20 de febrero. El Responsable del Sistema tiene la función de asegurar que dichas medidas de protección se llevan a cabo de forma efectiva en la Organización.

PROHIBICIÓN DE REPRESALIAS O CONDUCTAS PERJUDICIALES

Todo miembro de DOVALUE tiene completamente prohibido adoptar represalias frente a Informantes de buena fe, incluidas las amenazas de represalia y las tentativas de represalia.

Se entiende por **represalia** todo acto u omisión, así como cualquier trato adverso o conducta perjudicial, que estén prohibidos por la ley o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que los sufren en desventaja particular respecto de otra en el contexto laboral o profesional, por su condición de Informantes o Terceros relacionados, o por haber realizado una revelación pública.

A los efectos del artículo 36.2 de la Ley 2/2023, los actos perjudiciales que sufra el Informante dentro de los dos años siguientes a la comunicación o revelación se presumirán represalias, salvo prueba en contrario por parte de DOVALUE y sus filiales. En todo procedimiento corresponderá a La Compañía acreditar que la medida adoptada se fundó en motivos debidamente justificados y ajenos a la comunicación.

Se adjunta como **Anexo 2** un listado ejemplificativo, no limitativo, de acciones o actos encuadrables en la definición de represalia.

Si La Compañía tienen conocimiento de que se está produciendo o se ha producido una represalia, este tomará medidas razonables para detenerla y abordarla. En este sentido, se procederá a la remediación de la situación del Informante o el Tercero relacionado a la situación correspondiente de no haber sufrido la represalia o conducta perjudicial. Por ejemplo:

- Reintegrar a la persona en el mismo cargo o equivalente, con igual salario, responsabilidades, posición laboral y reputación;
- Permitir el acceso equitativo a la promoción, la capacitación, las oportunidades, los beneficios y los derechos;
- Restaurar a la persona a la posición mercantil anterior en relación con la Organización;
- Cesar o retirar el eventual conflicto o disputa interna que pudiera existir frente a la persona (por ejemplo, la actitud o el trato ofrecido);
- Pedir disculpas por cualquier perjuicio sufrido;
- Otorgar una indemnización por daños.

CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES

DOVALUE tiene la obligación de preservar la identidad del Informante y los Terceros relacionados, así como de garantizar un tratamiento confidencial de sus datos.

A este respecto, el Sistema interno de información está diseñado, establecido y gestionado de una forma segura, de modo que se garantice la confidencialidad de la identidad del Informante y de cualquier tercero mencionado en la Comunicación, y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la protección de datos, impidiendo el acceso de personal no autorizado.

La Compañía se compromete a no realizar tratamiento de datos de carácter personal que no resulten necesarios para el conocimiento de las acciones u omisiones advertidas en las comunicaciones inadecuadas en el Sistema interno de información y que no se encuentren, además, con la justificación legal oportuna; procediéndose, en ese caso, a su supresión.

Asimismo, la Compañía se compromete al cumplimiento de los plazos establecidos en la normativa aplicable y en el *Procedimiento corporativo de gestión del Sistema interno de información*. En particular, los datos personales relativos a las Comunicaciones y a las investigaciones internas se conservarán únicamente durante el período necesario y proporcionado; transcurridos tres (3) meses desde la recepción de la Comunicación sin que se hubieran iniciado actuaciones de investigación se procederá a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del Sistema, en cuyo caso constarán de forma anonimizada, sin que en ningún caso puedan conservarse por un período superior a diez (10) años.

10.4. MEDIDAS DE PROTECCIÓN A LAS PERSONAS AFECTADAS POR LA COMUNICACIÓN

De conformidad con el artículo 39 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 las principales medidas de

protección que se implementarán sobre las Personas afectadas por la Comunicación son las siguientes:

- Derecho a la presunción de inocencia: las personas afectadas por la Comunicación nunca podrán ser penalizada sin que se compruebe, previamente, la veracidad de los hechos contenidos en la Comunicación.
- Derecho de defensa: se concede a las personas implicadas la oportunidad de ofrecer una explicación a la situación comunicada, citándose para una entrevista o pidiendo aclaraciones destinadas al esclarecimiento de los hechos.
- Derecho de acceso al expediente: la Persona afectada por la Comunicación deberá ser informada de las acciones u omisiones que se le atribuyen. El derecho de acceso al expediente estará limitado por el respeto de las garantías de confidencialidad y protección de la identidad del Informante que la Ley 2/2023 consagra en su artículo 31. Esta información será aportada dentro de un plazo razonable, en los términos dispuestos por el art. 9.2.f, de manera que se atienda al “tiempo y forma que se considere adecuado” para garantizar el buen fin de la investigación.
- Protección de su identidad, garantizándose la confidencialidad de los hechos y datos del procedimiento.
- Cumplimiento de plazos: cumplimiento con los plazos establecidos en la normativa aplicable y en el *Procedimiento corporativo de gestión del Sistema interno de información*. Dichos plazos se detallan en el apartado 10.5 de la presente Política.

El alcance de estas medidas estará limitado por las especificidades que, en función de cada tipo de Comunicación o de su materia, resulten de aplicación en virtud de la normativa legal vigente.

10.5. CUMPLIMIENTO DE PLAZOS

La Organización gestionará las Comunicaciones recibidas respetando los plazos establecidos en la normativa aplicable, en particular en la Ley 2/2023, y en el *Procedimiento corporativo de gestión del Sistema interno de información*. Los plazos principales son los siguientes:

- Acuse de recibo: se remitirá al informante en el plazo máximo de siete (7) días naturales siguientes a la recepción de la Comunicación, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.
- Respuesta y cierre del expediente: la respuesta al informante sobre las actuaciones de investigación y el cierre del expediente se producirán en el plazo máximo de tres (3) meses desde la recepción de la Comunicación o, cuando no se hubiera remitido acuse de recibo, desde el vencimiento del plazo de siete (7) días naturales siguiente a su presentación. Cuando resulte procedente, se informará igualmente del cierre a la Persona afectada por la Comunicación, respetando en todo momento las obligaciones de confidencialidad y de protección de datos personales.
- Prórroga: en casos de especial complejidad que requieran una ampliación, el plazo podrá extenderse hasta un máximo de otros tres (3) meses adicionales. La prórroga será motivada, quedará documentada en el expediente y se notificará al informante.

Lo anterior se entiende sin perjuicio del plazo previsto para la celebración de la reunión presencial, recogido en el apartado 8.1.2, y de los plazos de conservación y supresión de los datos personales, recogidos en el apartado 10.3.

10.6. ACTIVACIÓN DE LA PROTECCIÓN

Las medidas de protección al Informante, los Terceros relacionados y las Personas afectadas por la Comunicación se activarán y darán comienzo tan pronto como se reciba la misma, y continuará durante e incluso después - cuando sea preciso- de la conclusión del proceso de investigación o gestión de la Comunicación.

11. CONSECUENCIAS DEL INCUMPLIMIENTO

Todas las personas a las que alcanza el presente documento tienen la obligación de cumplir con su contenido. En caso de identificarse un incumplimiento del mismo este podrá y deberá ser puesto en conocimiento del Responsable del Sistema a través de su Sistema interno de Información.

Cuando se confirme la contravención de lo indicado por estos textos, se adoptarán las medidas correspondientes, incluyendo las disciplinarias (en el ámbito laboral) o contractuales (en las relaciones mercantiles con Terceros) que consideren proporcionales al riesgo o daños ocasionados.

Las medidas que se adopten desde una perspectiva laboral serán respetuosas con la normativa aplicable, y se ajustarán, en función de la naturaleza y gravedad de los hechos, al régimen disciplinario interno, al Convenio Colectivo que resulte de aplicación y, en su defecto, al Estatuto de los Trabajadores, sin que por ello pierdan contundencia o proporcionalidad respecto de la conducta cometida. Cuando proceda, se informará asimismo a los Representantes Legales de los Trabajadores.

12. FORMACIÓN

doValue garantizará que todas las personas comprendidas en el ámbito subjetivo del Sistema Interno de Información reciban formación adecuada sobre su existencia y funcionamiento.

Dicha formación incluirá, al menos: las vías de acceso al canal y las infracciones que pueden ser objeto de comunicación, las garantías de confidencialidad y de protección frente a represalias de las que goza el Informante, la posibilidad de realizar comunicaciones anónimas, la existencia de canales externos de información (Autoridad Independiente de Protección del Informante, A.A.I.), el deber de confidencialidad y la tipificación como infracción muy grave de su quebranto conforme a la Ley 2/2023, la obligación de remitir de forma inmediata cualquier comunicación recibida por vía distinta al canal a cualquiera de los miembros del CSII, preservando la confidencialidad, y las consecuencias de la presentación de comunicaciones que se acrediten falsas o realizadas de mala fe.

Las acciones formativas se impartirán de forma periódica y se actualizarán cuando se produzcan cambios normativos o modificaciones relevantes en el Sistema. De todas las acciones formativas realizadas se dejará constancia documental.

13. PUBLICIDAD

La presente Política se entrega y está a disposición de todos los Miembros de la Organización, Socios de negocio y Terceros mediante su publicación en la página web de la Organización, en una sección separada y fácilmente identificable de la página principal:

<https://dovalue.es/>

<https://team4collection.com/>

Así como, aparece publicada en la intranet de intranet de DOVALUE:
www.doconnect.dovalue.it

La Compañía se comprometen a dar difusión y poner en conocimiento de todos los Miembros de la Organización la información necesaria para conocer el Sistema interno de información de la Organización, sus principios, garantías y obligaciones, así como su finalidad preventiva.

ANEXOS

ANEXO 1. Plantilla Modelo de Formulación de Comunicación

COMUNICACIÓN DE INFRACCIÓN NORMATIVA

Nombre del Informante (o, en su caso, "Anónimo"):

Área o Departamento (en caso de querer identificarse):

Persona afectada por la Comunicación (o denunciado):

Fecha de comisión de los hechos:

Hechos:

Pruebas que se aportan con la Comunicación:

Eventuales testigos de los hechos:

Firma del Informante y fecha:

ANEXO 2. Listado ejemplificativo de conductas consideradas represalias.

- Despido, suspensión, destitución o medidas equivalentes relacionadas con el contrato de trabajo, disciplinarias o afecten a la carrera profesional;
- Terminación anticipada o anulación de contratos de bienes o servicios;
- No renovación o terminación anticipada de un contrato de trabajo temporal;
- Cambio de puesto de trabajo o de funciones, cambio de ubicación del lugar de trabajo, reducción salarial o cambio del horario de trabajo u otras condiciones laborales;
- Degradación o denegación de ascensos;
- Evaluación o referencias negativas sobre el desempeño laboral o profesional;
- Imposición de cualquier medida disciplinaria, amonestación u otra sanción, incluidas las sanciones pecuniarias;
- Denegación de servicios;
- Denegación de formación;
- Daños, incluidos a su reputación, en especial en los medios sociales, o pérdidas económicas, incluidas la pérdida de negocio y de ingresos;
- Cualquier tipo de acto, intencionado o imprudente, que cause daño, físico o psicológico;
- Referencias médicas o psiquiátricas;
- Evaluación o referencias negativas con respecto a sus resultados laborales;
- Coacciones, intimidaciones, acoso u ostracismo o aislamiento;
- Discriminación, o trato desfavorable o injusto;

- Inclusión en listas negras sobre la base de un acuerdo sectorial, informal o formal, que pueda implicar que en el futuro la persona no vaya a encontrar empleo en dicho sector;
- Divulgación de la identidad del Informante;
- Pérdida financiera;
- Anulación o denegación de una licencia o permiso.