



STRATESYS TECHNOLOGY SOLUTIONS, S.L.

POLÍTICA Y PROTOCOLO DEL SISTEMA INTERNO DE INFORMACIÓN

(Canal de Denuncias – Ley 2/2023, de 20 de febrero)

Documento único que integra la Política del Sistema Interno de Información y el Protocolo del Buzón de Denuncias.

Versión refundida – **Junio 2026**

1. Introducción y objeto

El presente documento integra, en un texto único, la Política del Sistema Interno de Información y el Protocolo del Buzón de Denuncias de STRATESYS TECHNOLOGY SOLUTIONS, S.L. (en adelante, indistintamente, “STRATESYS” o la “Empresa”), y se adopta en desarrollo del Código de Conducta de STRATESYS y en cumplimiento 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 (en adelante, la “Ley 2/2023”), que transpone al ordenamiento español la Directiva (UE) 2019/1937.

Su finalidad es doble: (i) establecer un medio y un procedimiento directos, eficaces y confidenciales para detectar y comunicar potenciales incumplimientos legales, infracciones del Derecho de la Unión Europea y conductas contrarias al Código de Conducta o a la normativa interna; y (ii) otorgar protección adecuada frente a represalias a quienes informen de buena fe, fortaleciendo la cultura de integridad y cumplimiento de la organización.

Todos los directivos/as y empleados/as de STRATESYS quedan obligados por las normas internas en materia de información y denuncias contenidas en este documento.

2. Ámbito de aplicación y personas protegidas

2.1. Ámbito objetivo

El Sistema Interno de Información permite comunicar acciones u omisiones que puedan constituir: (i) infracciones del Derecho de la Unión Europea comprendidas en el ámbito de la Directiva (UE) 2019/1937 o que afecten a los intereses financieros de la Unión; (ii) infracciones penales o administrativas graves o muy graves, incluidas en todo caso las que impliquen quebranto económico para la Hacienda Pública o para la Seguridad Social; y (iii) incumplimientos del Código de Conducta, de la normativa interna o de la legislación vigente, así como irregularidades financieras o contables, por parte de empleados, directivos o administradores de STRATESYS, o de terceros que contraten con la Empresa (proveedores, clientes, administraciones públicas, accionistas, entre otros).

2.2. Ámbito subjetivo y personas protegidas

Podrá utilizar el Sistema cualquier persona física que, en un contexto laboral o profesional, haya obtenido información sobre las infracciones señaladas, conforme al artículo 3 de la Ley 2/2023, incluyendo: empleados/as; trabajadores/as por cuenta propia; accionistas, partícipes y miembros del órgano de administración, dirección o supervisión; personas que trabajen bajo la supervisión de contratistas, subcontratistas y proveedores; así como voluntarios, becarios, personas en formación, candidatos en procesos de selección o negociación precontractual y personas cuya relación laboral haya finalizado.

La protección frente a represalias se extiende igualmente a quienes asistan al informante, a personas de su entorno que puedan sufrir represalias y a los representantes legales de las personas trabajadoras en el ejercicio de sus funciones.

Comunicaciones de mala fe. Queda rigurosamente prohibido formular comunicaciones o denuncias infundadas, inciertas o falsas. Quien comunique o revele información a sabiendas de su falsedad no gozará de la protección prevista en este documento ni en la Ley 2/2023, sin perjuicio de las responsabilidades de toda índole en que pudiera incurrir.

3. Principios de actuación

La actuación del Sistema Interno de Información se rige por los siguientes principios:

- Perseguir los más altos estándares de transparencia, ética y responsabilidad, promoviendo la tolerancia cero frente a actuaciones irregulares y la lucha contra la corrupción.
- Respetar la legislación vigente aplicable a la actividad de la Empresa y, en particular, su normativa interna.
- Impulsar la implicación del personal en la prevención y detección de actos ilícitos mediante la formación y la difusión del canal interno como medio de comunicación de conductas contrarias a la legalidad.
- Garantizar la independencia y autonomía funcional del Responsable del Sistema, dotándolo de los medios personales y materiales necesarios para el desempeño eficaz de su función.
- Reaccionar de forma pronta y eficaz ante cualquier comunicación, investigándola con respeto a los derechos del informante y de las personas afectadas, evitando medidas desproporcionadas o discriminatorias.
- Garantizar la confidencialidad de la identidad del informante, de las personas afectadas y de cualquier tercero mencionado, así como la presunción de inocencia y el derecho de defensa de la persona afectada.
- Poner en conocimiento de las autoridades competentes los presuntos delitos, ofreciendo plena cooperación. El Responsable del Sistema remitirá la información al Ministerio Fiscal con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito, o a la Fiscalía Europea cuando afecten a los intereses financieros de la Unión Europea.

4. Responsable del Sistema Interno de Información

4.1. Designación y naturaleza

El órgano de administración de STRATESYS, previa consulta con la representación legal de las personas trabajadoras, es el competente para la implantación del Sistema Interno de Información, para la designación y, en su caso, cese del Responsable del Sistema, y para la

aprobación del procedimiento de gestión de informaciones. El órgano de administración tiene la condición de responsable del tratamiento de los datos personales derivados del Sistema.

El Responsable del Sistema Interno de Información (en adelante, el “Responsable del Sistema”) es el garante del funcionamiento del canal y de la protección frente a represalias. Sin perjuicio de lo previsto en el apartado 4.3, la función recae en Cumplimiento Normativo, que será el destinatario en primer lugar de toda comunicación o denuncia. El Responsable del Sistema desarrollará sus funciones de forma independiente y autónoma respecto del resto de órganos de la Empresa, no podrá recibir instrucciones de ningún tipo en su ejercicio y reportará directamente al órgano de administración.

El nombramiento y el cese del Responsable del Sistema — y, en su caso, de los integrantes del órgano colegiado — se notificarán a la Autoridad Independiente de Protección del Informante, A.A.I. (o, en su caso, a la autoridad autonómica competente), en el plazo de los diez días hábiles siguientes, especificando en el caso de cese las razones que lo justifican.

4.2. Comité de Cumplimiento Normativo

El Responsable del Sistema pondrá en conocimiento del Comité de Cumplimiento Normativo, de forma periódica y al menos trimestralmente, la relación de comunicaciones recibidas, las investigaciones realizadas, su resultado y, en su caso, las medidas adoptadas. En función del área de negocio afectada, podrá recabarse información adicional del responsable del área, exclusivamente para el tratamiento del asunto concreto de que se trate.

4.3. Suplencia temporal del Responsable del Sistema

En los supuestos de ausencia, vacante, enfermedad, abstención por conflicto de interés o cualquier otra imposibilidad temporal del Responsable del Sistema, sus funciones serán asumidas con carácter transitorio por un comité de suplencia integrado por dos (2) personas, compuesto por la responsable del Departamento Legal y la dirección Financiera (CFO).

Esta previsión se ampara en el artículo 8.2 de la Ley 2/2023, que admite expresamente que el Responsable del Sistema sea un órgano colegiado, y responde a la recomendación de que el órgano de administración tenga preestablecido un régimen de suplencias que asegure la continuidad del Sistema. La suplencia se regirá por las siguientes reglas:

- El comité de suplencia delegará en uno de sus dos miembros las facultades de gestión del Sistema Interno de Información y de tramitación de los expedientes de investigación, a fin de preservar la atribución personal de responsabilidad exigida por la Ley. El otro miembro actuará como apoyo y suplente de aquél.
- Ambos integrantes desarrollarán sus funciones con la misma independencia y autonomía funcional exigidas al Responsable del Sistema, sin recibir instrucciones de ningún órgano de la Empresa, y quedarán sujetos a idénticos deberes de confidencialidad y de abstención en caso de conflicto de interés.
- La activación del régimen de suplencia y la identidad de los miembros del comité, así como la delegación de facultades prevista en el primer guion, se notificarán a la Autoridad Independiente de Protección del Informante (o autoridad autonómica competente) dentro de los diez días hábiles siguientes, conforme al artículo 8.3 de la Ley 2/2023.

- La suplencia tendrá carácter exclusivamente temporal y cesará automáticamente al reincorporarse el Responsable del Sistema o al designarse uno nuevo por el órgano de administración.

5. Formulación de comunicaciones y denuncias

5.1. Canales disponibles

El canal interno permite presentar comunicaciones por escrito, verbalmente o de ambas formas, siendo el cauce preferente para informar sobre las conductas comprendidas en el apartado 2.1:

- Buzón de Denuncias electrónico: a través del enlace al Portal de Denuncias habilitado al efecto, accesible desde la página de inicio del sitio web corporativo.
- Por escrito: mediante correo postal o cualquier otro medio electrónico habilitado dirigido al Responsable del Sistema.
- Verbalmente: por vía telefónica o sistema de mensajería de voz y, a solicitud del informante, mediante reunión presencial dentro del plazo máximo de siete (7) días. Las comunicaciones verbales se documentarán mediante grabación en formato seguro y accesible o mediante transcripción completa y exacta, previa información al informante.

El sistema interno de información es el cauce preferente, sin perjuicio del derecho del informante a acudir directamente al canal externo de la Autoridad Independiente de Protección del Informante (o autoridad autonómica competente), conforme se indica en el apartado 8.

5.2. Contenido y forma

El informante proporcionará toda la información de que disponga para facilitar el análisis del hecho comunicado. Se procurará que las comunicaciones sean nominativas, sin perjuicio de que el Sistema admite y tramita comunicaciones anónimas. Cuando la comunicación sea nominativa o permita la respuesta, se confirmará su recepción conforme al apartado 6.

6. Tramitación de las comunicaciones

6.1. Registro

El Responsable del Sistema llevará un libro-registro de todas las comunicaciones recibidas y de las investigaciones internas a que den lugar. Este registro no será público y se gestionará conforme a la normativa de protección de datos. Solo se accederá a su contenido en los términos legalmente previstos.

6.2. Acuse de recibo

Se remitirá acuse de recibo de la comunicación al informante en el plazo máximo de siete (7) días naturales siguientes a su recepción, salvo que el informante haya renunciado a recibirlo o que ello pueda poner en peligro la confidencialidad de la comunicación.

6.3. Admisión y primera valoración

Recibida la comunicación, el Responsable del Sistema verificará si los hechos se encuentran dentro del ámbito objetivo y subjetivo del Sistema y realizará una primera valoración motivada. En función de la naturaleza de los hechos, podrá poner la comunicación en conocimiento del superior jerárquico responsable del empleado/a afectado/a, con las debidas cautelas de confidencialidad.

Cuando el Responsable del Sistema considere que la comunicación carece manifiestamente de fundamento, dejará constancia en el registro y adoptará decisión escrita y motivada de no iniciar investigación, que pondrá en conocimiento del Comité de Cumplimiento Normativo. Ello no impedirá la iniciación de una investigación posterior si se recibe información nueva y adicional.

6.4. Instrucción e investigación

El Responsable del Sistema realizará las investigaciones internas que estime necesarias para el esclarecimiento de los hechos, respetando los principios de este documento. Podrá recabar de cualquier empleado, área o departamento la información y documentación que considere oportuna, y solicitar la colaboración de las áreas relacionadas con los hechos.

Atendida la naturaleza, características o gravedad de los hechos, el Responsable del Sistema podrá recabar el asesoramiento de letrados externos u otros expertos y, previa autorización del Comité de Cumplimiento Normativo, externalizar la investigación a profesionales especializados, siempre con sujeción a los deberes de confidencialidad.

6.5. Derechos de la persona afectada

La persona afectada tiene derecho a la presunción de inocencia, a ser informada de las acciones u omisiones que se le atribuyen y a ser oída en cualquier momento, así como al acceso al expediente en los términos legalmente previstos, salvo cuando dicho conocimiento pudiera facilitar la ocultación, destrucción o alteración de pruebas. El tratamiento de sus datos se ajustará a la normativa de protección de datos.

6.6. Plazo de resolución

El plazo máximo para dar respuesta a las actuaciones de investigación no podrá ser superior a tres (3) meses, computados desde la recepción de la comunicación o, si no se hubiera remitido acuse de recibo, desde el vencimiento del plazo de siete (7) días naturales posteriores a la presentación de la comunicación. En casos de especial complejidad, debidamente motivados, el plazo podrá ampliarse por otros tres (3) meses adicionales, informando de ello al informante.

6.7. Informe final y decisión

Finalizada la investigación, el Responsable del Sistema convocará al Comité de Cumplimiento Normativo para la evaluación de los hechos y la formulación de un informe final escrito con sus conclusiones. Dicho informe se trasladará al Consejo de Administración, órgano competente para adoptar las decisiones o acciones procedentes con arreglo a la normativa laboral vigente y al convenio colectivo aplicable, sin perjuicio de otras responsabilidades administrativas o penales que pudieran concurrir.

Se comunicará al informante el resultado de las actuaciones dentro del plazo previsto en el apartado 6.6, con el alcance que permita la salvaguarda de la confidencialidad y de los datos de terceros.

7. Confidencialidad, protección frente a represalias y datos personales

7.1. Confidencialidad y anonimato

Se garantiza en todo momento la confidencialidad de la identidad del informante, de las personas afectadas y de los terceros mencionados, así como de las actuaciones de gestión y tramitación. La identidad del informante únicamente podrá revelarse en los supuestos legalmente previstos (entre otros, a la autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente). El Sistema admite y tramita comunicaciones anónimas.

7.2. Prohibición de represalias

Se proporcionará protección a todas las personas que realicen una comunicación de buena fe conforme a este procedimiento. Queda prohibida cualquier forma de represalia, directa o indirecta, contra el informante o las personas protegidas. Los actos que constituyan represalia serán nulos de pleno derecho y darán lugar a las medidas disciplinarias o de responsabilidad que procedan, sin perjuicio de la correspondiente indemnización de daños y perjuicios.

7.3. Protección de datos personales

El tratamiento de datos personales derivado del Sistema se regirá por el Reglamento (UE) 2016/679 (RGPD), la Ley Orgánica 3/2018 (LOPDGDD) y la Ley 2/2023, aplicando los principios de minimización, limitación de la conservación y control estricto de accesos. Los datos se conservarán únicamente durante el tiempo necesario y proporcionado y, en todo caso, conforme al artículo 32 de la Ley 2/2023; transcurridos tres (3) meses desde la recepción sin que se hayan iniciado actuaciones de investigación, los datos se suprimirán del Sistema, sin perjuicio de su eventual bloqueo o conservación fuera del canal cuando sea necesario para acreditar el funcionamiento del modelo o atender posibles responsabilidades.

8. Canal externo de información

Con independencia del canal interno, toda persona podrá dirigirse directamente al canal externo de la Autoridad Independiente de Protección del Informante, A.A.I. (adscrita al Ministerio de Justicia), o a las autoridades u órganos competentes de las comunidades autónomas, ya sea de forma directa o tras haber comunicado a través del canal interno. STRATESYS facilitará información clara y accesible sobre la existencia y forma de acceso a los canales externos.

9. Evaluación, revisión y control

El Responsable del Sistema goza de las facultades de iniciativa y control para evaluar y supervisar la eficacia del canal interno, reportar sobre su cumplimiento efectivo y proponer

mejoras. Le corresponde controlar y supervisar la correcta implantación y el cumplimiento del Sistema como máximo garante del mismo.

Si de una comunicación se evidenciara la necesidad de reforzar, adaptar o modificar los controles internos, el Responsable del Sistema lo pondrá en conocimiento del Comité de Cumplimiento Normativo para formular conjuntamente la propuesta correspondiente. Toda propuesta de adaptación, reforzamiento o modificación de cualquier protocolo de cumplimiento interno se someterá al Consejo de Administración, único órgano competente y responsable de las decisiones últimas sobre la normativa de cumplimiento de STRATESYS.

10. Difusión, aprobación y vigencia

STRATESYS garantizará que el presente documento sea difundido y que exista conocimiento actualizado del mismo entre todo su personal, así como su accesibilidad para los terceros legitimados. El canal interno será accesible desde la página de inicio del sitio web corporativo.

El presente documento refunde e integra la Política del Sistema Interno de Información y el Protocolo del Buzón de Denuncias, aprobados por el Comité de Cumplimiento con fecha 15 de julio de 2022 y actualizados el 20 de mayo de 2024.

La presente versión refundida ha sido aprobada por el órgano de administración de STRATESYS en junio de 2026 y queda a disposición de todo el personal para su conocimiento.