

POLÍTICA Y PROTOCOLO DEL SISTEMA INTERNO DE INFORMACIÓN

España · Stratesys Technology Solutions, S.L.

Confidencialidad · Independencia · Protección · Diligencia

Versión	2.0
Última actualización	Agosto de 2026
Ámbito	España
Entidad	Stratesys Technology Solutions, S.L.
Aprobación	Órgano de administración

Documento corporativo de acceso público

CONTENIDO

1. Objeto, naturaleza y marco normativo
2. Ámbito de aplicación
3. Principios y garantías
4. Estructura y responsabilidades
5. Presentación de comunicaciones
6. Gestión de las informaciones
7. Investigación y derechos de la persona afectada
8. Conclusión y medidas
9. Protección del informante y prohibición de represalias
10. Canales externos de información
11. Protección de datos, seguridad y libro-registro
12. Información, formación, revisión y vigencia

Documentos relacionados

Documento integrado: Este texto reúne la Política del Sistema Interno de Información y su procedimiento de gestión. Se aplica al sistema español y no incorpora el procedimiento específico de Portugal.

1. Objeto, naturaleza y marco normativo

La presente Política y Protocolo regula el Sistema Interno de Información de STRATESYS TECHNOLOGY SOLUTIONS, S.L. (en adelante, «STRATESYS»), incluido su canal interno, la figura del Responsable del Sistema y el procedimiento de gestión de las informaciones.

Su objeto es facilitar la comunicación segura de posibles infracciones, permitir su análisis diligente, proteger a quienes informen en las condiciones legalmente previstas y reforzar la cultura de integridad de STRATESYS. El Sistema constituye una herramienta de detección y respuesta, sin sustituir los cauces laborales, de recursos humanos, de seguridad o de atención comercial que correspondan por razón de la materia.

1.1 Marco normativo

El documento se interpreta conforme a la Ley 2/2023, de 20 de febrero; la Directiva (UE) 2019/1937; el Reglamento (UE) 2016/679; la Ley Orgánica 3/2018, de 5 de diciembre; y la normativa laboral, penal y sectorial aplicable.

1.2 Implantación y aprobación

El órgano de administración es responsable de la implantación del Sistema, previa consulta con la representación legal de las personas trabajadoras, y aprueba esta Política y el procedimiento de gestión. La gestión corresponde al Responsable del Sistema con independencia y autonomía.

Interpretación: La protección establecida por la Ley 2/2023 se aplica cuando concurren sus requisitos. STRATESYS podrá tramitar también otros incumplimientos éticos o internos, aunque su protección jurídica se determinará según el caso y la normativa aplicable.

2. Ámbito de aplicación

2.1 Ámbito material

Podrán comunicarse acciones u omisiones conocidas en un contexto laboral o profesional que puedan constituir:

- infracciones del Derecho de la Unión Europea comprendidas en el ámbito de la Ley 2/2023, incluidas las que afecten a sus intereses financieros o incidan en el mercado interior;
- infracciones penales o administrativas graves o muy graves, incluidas las que impliquen quebranto económico para la Hacienda Pública o la Seguridad Social;
- infracciones en materia de seguridad y salud en el trabajo comprendidas en el ámbito legal de protección; y
- incumplimientos del Código de Conducta, de la Política de Prevención de Delitos o de otras normas internas de STRATESYS.

2.2 Personas que pueden informar

Podrá utilizar el Sistema cualquier persona que haya obtenido la información en un contexto laboral o profesional, entre otras:

- personas trabajadoras, antiguas trabajadoras y candidatas durante procesos de selección o negociación precontractual;
- personas autónomas, accionistas, partícipes y miembros del órgano de administración, dirección o supervisión;
- personas que trabajen para o bajo la supervisión y dirección de contratistas, subcontratistas y proveedores;
- voluntariado, becarios y personas en formación, con independencia de que perciban remuneración.

La protección podrá extenderse, en los términos de la Ley 2/2023, a facilitadores, representantes legales de las personas trabajadoras, personas relacionadas con el informante que puedan sufrir represalias y determinadas personas jurídicas vinculadas.

2.3 Comunicaciones ajenas al Sistema

Las consultas generales, reclamaciones de clientes, incidencias de servicio, conflictos estrictamente interpersonales sin posible infracción y emergencias deberán dirigirse a los cauces específicos. Si una comunicación recibida no pertenece al ámbito del Sistema, se informará al remitente cuando sea posible y se orientará al canal adecuado, sin divulgar su identidad de forma indebida.

3. Principios y garantías

- Accesibilidad: presentación por escrito o verbalmente, de manera identificada o anónima.
- Confidencialidad: protección de la identidad del informante, de la persona afectada y de terceros mencionados.
- Independencia y ausencia de conflictos de interés en la recepción, análisis e investigación.
- Prohibición de represalias y protección de quienes informen con motivos razonables para considerar veraz la información.
- Presunción de inocencia, derecho de defensa, audiencia, honor y buena reputación de la persona afectada.
- Diligencia, objetividad, proporcionalidad, minimización de datos y trazabilidad de las actuaciones.

4. Estructura y responsabilidades

4.1 Órgano de administración

Corresponde al órgano de administración implantar el Sistema, aprobar la Política y el procedimiento, designar y cesar al Responsable del Sistema, asegurar recursos suficientes y recibir información agregada sobre su funcionamiento. No interviene en la gestión ordinaria de los expedientes ni accede a identidades o detalles salvo que sea imprescindible para ejercer una competencia legal o adoptar una decisión, aplicando estrictamente el principio de necesidad.

4.2 Responsable del Sistema

El Responsable del Sistema es la persona física u órgano colegiado designado por el órgano de administración. Si se designa un órgano colegiado, este delegará en uno de sus miembros las facultades de gestión y tramitación. Actúa con independencia y autonomía, sin recibir instrucciones en el ejercicio de sus funciones.

Le corresponde, entre otras funciones, recibir y registrar informaciones; decidir sobre su admisión; mantener la comunicación con el informante; dirigir o supervisar la investigación; adoptar medidas de protección y cautelares dentro de sus competencias; resolver o formular las propuestas que procedan; custodiar el libro-registro; y reportar datos agregados sobre el funcionamiento del Sistema.

Su nombramiento y cese se comunicarán a la Autoridad Independiente de Protección del Informante, A.A.I., o a la autoridad autonómica competente, en los plazos legalmente exigibles.

4.3 Comité de Cumplimiento Normativo

El Comité de Cumplimiento Normativo supervisa el modelo de cumplimiento penal y puede recibir información estadística o anonimizada, proponer mejoras de controles y prestar apoyo técnico cuando lo solicite el Responsable del Sistema. No sustituye al Responsable, no autoriza la tramitación de expedientes y no accede a la identidad del informante ni al contenido íntegro de un caso salvo necesidad justificada, habilitación legal y ausencia de conflicto.

4.4 Apoyo especializado, proveedor externo y conflictos

El Responsable podrá recabar apoyo de Legal, Recursos Humanos, Seguridad de la Información, Auditoría u otros expertos, internos o externos, limitando el acceso a lo estrictamente necesario. La plataforma Centinela actúa como soporte tecnológico y canal de entrada, sin asumir por ello la condición ni las decisiones propias del Responsable del Sistema.

Toda persona con un conflicto real o potencial se abstendrá. El expediente será reasignado al suplente o a la persona independiente previamente designada. Si el conflicto afecta al Responsable del Sistema, se activará el mecanismo de suplencia aprobado por el órgano de administración y se cumplirán, cuando proceda, las obligaciones de comunicación a la autoridad competente.

5. Presentación de comunicaciones

5.1 Canal interno: Centinela

El Portal de Denuncias Centinela es el punto corporativo de acceso al canal interno de STRATESYS y permite presentar y realizar el seguimiento seguro de comunicaciones. El acceso estará disponible de forma clara en el sitio web corporativo.

[ACCEDER AL PORTAL DE DENUNCIAS – CENTINELA]

La comunicación podrá efectuarse por escrito o verbalmente a través de las funcionalidades habilitadas. A solicitud del informante, también podrá celebrarse una reunión presencial dentro del plazo máximo de siete días. STRATESYS facilitará, cuando sea necesario, un cauce telefónico, de mensajería de voz, postal o equivalente que preserve las mismas garantías.

5.2 Anonimato, seguimiento y reunión

Las comunicaciones pueden ser anónimas. El informante deberá conservar las credenciales o el código facilitado por la plataforma para consultar mensajes y aportar información adicional. La falta de identificación no impedirá la tramitación si existen datos suficientes.

Las comunicaciones verbales se documentarán, previo aviso y consentimiento cuando sea exigible, mediante grabación en formato seguro o transcripción completa y exacta. El informante podrá comprobar, rectificar y aceptar la transcripción mediante su firma.

5.3 Contenido recomendado

Se recomienda describir los hechos con claridad, indicar fechas, lugares, personas o áreas relacionadas y aportar documentos disponibles obtenidos lícitamente. No es necesario acreditar de forma concluyente la infracción, pero sí actuar con motivos razonables y sin fabricar, alterar u obtener ilícitamente pruebas.

Urgencias: Cuando exista un peligro inmediato para personas, bienes o sistemas, deberá contactarse además con los servicios de emergencia o con el área interna competente. El Canal no sustituye una respuesta urgente.

6. Gestión de las informaciones

6.1 Recepción, acuse y registro

Toda información recibida se incorporará de forma restringida al libro-registro. Se enviará acuse de recibo en un máximo de siete días naturales, salvo que el informante haya renunciado a recibir comunicaciones, la comunicación sea anónima sin posibilidad de seguimiento o el acuse pueda comprometer la confidencialidad.

6.2 Análisis preliminar y admisión

El Responsable comprobará el ámbito, la verosimilitud inicial, la existencia de datos suficientes, posibles conflictos de interés, riesgos de represalia y la necesidad de preservar pruebas. Podrá solicitar aclaraciones al informante por el canal seguro.

La admisión o inadmisión se documentará de forma motivada. Podrá inadmitirse, entre otros supuestos, cuando los hechos sean manifiestamente inverosímiles, ajenos al ámbito del Sistema, carezcan de datos mínimos tras solicitar aclaración, consistan en una mera reiteración sin información nueva o hayan sido obtenidos mediante la comisión de un delito. La inadmisión no impide reabrir el análisis si aparecen elementos nuevos.

6.3 Comunicación recibida por otro medio

Quien reciba una información fuera de los cauces habilitados deberá remitirla sin demora al Responsable del Sistema, abstenerse de investigar o difundirla y guardar absoluta confidencialidad. La quiebra de esta obligación podrá constituir una infracción muy grave conforme a la Ley 2/2023.

6.4 Plazos

Hito	Plazo o criterio
Acuse de recibo	Máximo de 7 días naturales desde la recepción, con las excepciones indicadas.
Respuesta	Máximo de 3 meses desde el acuse o, si no se envió, desde el vencimiento de los 7 días posteriores a la comunicación.
Ampliación	Hasta 3 meses adicionales en casos de especial complejidad, mediante decisión motivada.
Reunión solicitada	Dentro de los 7 días siguientes a la solicitud.

7. Investigación y derechos de la persona afectada

7.1 Plan de investigación

Admitida la comunicación, el Responsable definirá el objeto, las diligencias, las personas con acceso, el calendario y, en su caso, las medidas de preservación de pruebas y de protección. Las actuaciones serán pertinentes, proporcionadas y documentadas.

Podrán realizarse entrevistas, análisis documental o técnico y solicitudes de información. Los equipos de apoyo actuarán bajo deber de confidencialidad y con acceso limitado. Cuando resulte necesario, podrá contratarse asesoramiento externo especializado sin requerir autorización del Comité de Cumplimiento, sin perjuicio de los controles de contratación y protección de datos aplicables.

7.2 Derechos de la persona afectada

La persona afectada será informada de las acciones u omisiones que se le atribuyen y podrá ser oída en el tiempo y forma adecuados para garantizar su defensa sin perjudicar la investigación. Tendrá derecho a formular alegaciones y aportar pruebas, así como a la presunción de inocencia, al honor y a la confidencialidad.

No se le comunicará la identidad del informante ni se le reconocerá acceso a información que permita identificarlo. El acceso al expediente se limitará conforme a la ley y a los derechos de terceros. La audiencia podrá aplazarse de forma motivada mientras exista riesgo real de ocultación, destrucción o alteración de pruebas.

7.3 Medidas cautelares

Podrán proponerse o adoptarse medidas temporales para proteger a las personas, preservar evidencias, evitar represalias o impedir la continuidad del riesgo. Serán necesarias, idóneas, proporcionadas, revisables y no prejuzgarán el resultado.

8. Conclusión y medidas

Finalizada la investigación, el Responsable emitirá una decisión o informe motivado que describa, con el grado de detalle adecuado, los hechos analizados, diligencias practicadas, valoración y conclusión. Según el resultado, podrá acordar el archivo, recomendar medidas correctoras o disciplinarias, trasladar actuaciones al órgano competente o proponer mejoras de control.

Cuando los hechos pudieran ser indiciariamente constitutivos de delito, la información se remitirá de inmediato al Ministerio Fiscal. Si afectaran a los intereses financieros de la Unión Europea, se remitirán a la Fiscalía Europea. También se dará traslado a otras autoridades competentes cuando resulte legalmente exigible.

El informante recibirá información sobre la tramitación y su resultado dentro de los plazos aplicables, siempre que exista un medio seguro de contacto y con el alcance compatible con la confidencialidad, los derechos de terceros y las actuaciones posteriores. No se comunicarán datos disciplinarios, personales o reservados que no sean necesarios.

9. Protección del informante y prohibición de represalias

9.1 Condiciones de protección

Gozarán de protección quienes tengan motivos razonables para pensar que la información era veraz en el momento de comunicarla, aunque no aporten pruebas concluyentes, y la comunicación se encuentre dentro del ámbito de la Ley 2/2023. La protección alcanza también a las personas relacionadas previstas legalmente.

9.2 Represalias prohibidas

Se prohíben las represalias, amenazas y tentativas de represalia. Entre otras, pueden consistir en despido, suspensión, degradación, denegación de ascensos, cambios perjudiciales de funciones u horario, evaluaciones negativas, acoso, discriminación, daños reputacionales, inclusión en listas negras, resolución contractual o perjuicios económicos.

El informante podrá comunicar cualquier posible represalia al Responsable del Sistema, que evaluará medidas de protección y la trasladará al órgano competente solo en la medida necesaria. La protección no impide adoptar decisiones legítimas, debidamente justificadas y ajenas a la comunicación.

9.3 Comunicaciones deliberadamente falsas

La inexactitud o falta de prueba no determina por sí sola mala fe. Quien comunique información a sabiendas de su falsedad o manipule pruebas no gozará de protección por ese comportamiento y podrá incurrir en responsabilidad. Cualquier medida deberá respetar la legislación aplicable y las garantías del procedimiento.

10. Canales externos de información

El informante puede acudir al canal externo competente directamente o después de utilizar el canal interno. La utilización de Centinela no es obligatoria ni condiciona el acceso a las autoridades.

En el ámbito estatal, la Autoridad Independiente de Protección del Informante, A.A.I. dispone de un canal externo accesible desde su sede electrónica. También podrán resultar competentes autoridades autonómicas o autoridades sectoriales, nacionales o de la Unión Europea, atendiendo a la materia y al ámbito territorial.

[CANAL EXTERNO DE LA A.A.I. – SEDE ELECTRÓNICA]

Elección del canal: La persona informante puede elegir el cauce que considere más adecuado. STRATESYS anima a utilizar el canal interno cuando la infracción pueda tratarse eficazmente y no exista riesgo de represalia, sin limitar el derecho a acudir externamente.

11. Protección de datos, seguridad y libro-registro

11.1 Responsabilidad y finalidad

STRATESYS, a través de su órgano de administración, es responsable del tratamiento asociado al Sistema. Los datos se tratarán para recibir, analizar e investigar informaciones, adoptar medidas y cumplir las obligaciones legales. Los proveedores tecnológicos o investigadores externos actuarán conforme al rol y a las garantías que correspondan.

11.2 Acceso y minimización

El acceso se limitará al Responsable del Sistema y a quienes estén legalmente autorizados o deban intervenir de manera imprescindible. La identidad del informante solo podrá comunicarse a la autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en una investigación, con las salvaguardas previstas en la ley.

No se recopilarán datos manifiestamente irrelevantes y, si se obtienen por accidente, se suprimirán sin dilación indebida. Los datos de categorías especiales solo se tratarán cuando sea estrictamente necesario y exista habilitación suficiente.

11.3 Conservación

Los datos permanecerán en el propio Sistema únicamente durante el tiempo imprescindible para decidir si procede iniciar una investigación. Transcurridos tres meses desde su introducción, deberán suprimirse del Sistema; cuando sea necesario continuar la investigación, podrán conservarse en un entorno separado, seguro y con acceso restringido. Las comunicaciones no tramitadas solo podrán conservarse de forma anonimizada para evidenciar el funcionamiento del Sistema.

La documentación del expediente se conservará durante el tiempo necesario para atender las finalidades legítimas y responsabilidades aplicables, conforme a los plazos internos de conservación y bloqueo. Los datos se suprimirán de manera segura cuando dejen de ser necesarios.

11.4 Libro-registro y seguridad

Se mantendrá un libro-registro confidencial de las informaciones y de las investigaciones. No será público y su contenido únicamente podrá facilitarse total o parcialmente a petición razonada de la autoridad judicial competente, mediante auto y en el marco de un procedimiento judicial. Se aplicarán controles de acceso, cifrado, copias de seguridad, trazabilidad y gestión de incidentes adecuados al riesgo.

11.5 Derechos de protección de datos

Las personas interesadas podrán ejercer sus derechos conforme a la información de privacidad aplicable. El derecho de oposición se presumirá legítimamente limitado cuando sea necesario mantener el tratamiento para prevenir, detectar o investigar infracciones, sin perjuicio de la valoración individual que corresponda.

12. Información, formación, revisión y vigencia

12.1 Publicidad y formación

STRATESYS publicará información clara y accesible sobre el uso del canal interno, sus garantías y los canales externos. El personal recibirá formación proporcionada a sus funciones, especialmente quienes puedan recibir comunicaciones o participar en investigaciones.

12.2 Seguimiento

El Responsable del Sistema realizará un seguimiento periódico mediante indicadores agregados —por ejemplo, volumen, tipología, tiempos de tramitación y medidas de mejora— sin revelar identidades ni detalles innecesarios. Informará al órgano de administración y, en su ámbito, al Comité de Cumplimiento Normativo.

12.3 Revisión

El documento se revisará cuando se produzcan cambios normativos, organizativos o tecnológicos relevantes, incidentes significativos o conclusiones de auditoría que lo aconsejen y, en todo caso, de forma periódica. Las modificaciones sustanciales se someterán a aprobación del órgano de administración y, cuando corresponda, a consulta con la representación legal de las personas trabajadoras.

12.4 Aprobación y vigencia

Esta versión sustituye a las versiones anteriores de la Política del Sistema Interno de Información y del Protocolo del Buzón de Denuncias de STRATESYS. Entrará en vigor en la fecha de su aprobación por el órgano de administración y permanecerá vigente hasta su modificación o sustitución.

Nota de aprobación: Antes de su publicación deberá completarse en el registro corporativo la fecha exacta del acuerdo de aprobación y comprobarse la vigencia de los enlaces al Portal Centinela y al canal externo de la A.A.I.

DOCUMENTOS RELACIONADOS

- Código de Conducta de Stratesys.
- Política de Prevención de Delitos de Stratesys.
- Información de privacidad del Sistema Interno de Información.
- Información específica aplicable a Portugal — documento autónomo.
- Mapa de riesgos penales y controles asociados aplicables a la sociedad.

Estos documentos se relacionan con el Sistema, pero no es necesario incorporarlos físicamente como anexos a la versión pública de esta Política. Su aprobación, acceso y nivel de confidencialidad se regirán por su propia naturaleza.