

POLÍTICA DE PREVENCIÓN DE DELITOS

Grupo Stratesys

Cultura ética · Prevención · Detección · Respuesta

Versión	2.0
Última actualización	Agosto de 2026
Ámbito	Grupo Stratesys
Órgano responsable de aprobación	Órgano de administración u órgano competente de cada sociedad del Grupo

Documento corporativo de acceso público

CONTENIDO

1. Objeto, finalidad y marco normativo
2. Ámbito de aplicación
3. Principios generales
4. Gobernanza y responsabilidades
5. Integración en el Modelo de Prevención
6. Principales áreas de riesgo penal
7. Normas esenciales de conducta
8. Relaciones con terceros
9. Formación, información y asesoramiento
10. Sistema Interno de Información – Canal de Denuncias
11. Investigación y respuesta
12. Consecuencias del incumplimiento
13. Protección de datos y conservación
14. Seguimiento, revisión y entrada en vigor

Anexo. Documentos relacionados

Naturaleza del documento: Esta Política establece los principios y reglas generales de prevención penal del Grupo. No sustituye al mapa de riesgos, la matriz de controles, los protocolos de decisión, el régimen disciplinario ni el resto de documentos que integran el Modelo de Organización y Gestión.

1. Objeto, finalidad y marco normativo

El Grupo Stratesys mantiene un compromiso firme con el cumplimiento de la ley, la integridad empresarial y el desarrollo de su actividad conforme a principios éticos. Esta Política establece el marco general para prevenir, detectar y responder ante conductas que puedan constituir delitos o incumplimientos graves.

La Política forma parte del sistema de cumplimiento normativo y del Modelo de Organización y Gestión para la Prevención de Delitos de las sociedades del Grupo a las que resulte aplicable. Su finalidad no es garantizar la inexistencia absoluta de conductas ilícitas, sino establecer una organización y unos controles adecuados para reducir de forma significativa el riesgo de comisión y favorecer una verdadera cultura de cumplimiento.

1.1 Marco normativo

En España, esta Política se interpreta de conformidad con el Código Penal, en particular sus artículos 31 bis y siguientes, las reformas introducidas por las Leyes Orgánicas 5/2010 y 1/2015, la Ley 2/2023, de protección de las personas que informen sobre infracciones normativas, y las demás disposiciones aplicables.

En las restantes jurisdicciones se aplicará junto con la legislación local y con las adaptaciones o procedimientos específicos aprobados para cada sociedad. Cuando una norma local establezca garantías superiores o requisitos imperativos diferentes, prevalecerá dicha norma en su ámbito de aplicación.

1.2 Objetivos

- Promover una cultura corporativa basada en la integridad, la responsabilidad y el cumplimiento.
- Identificar y gestionar los riesgos penales vinculados a la actividad del Grupo.
- Establecer reglas de conducta claras para las Personas Sujetas y los terceros relacionados.
- Facilitar la comunicación segura de posibles infracciones y proteger a quienes informen conforme a la ley.
- Investigar y responder de manera diligente, independiente, proporcional y documentada.
- Revisar periódicamente la eficacia del sistema y adoptar medidas de mejora continua.

2. Ámbito de aplicación

2.1 Ámbito societario

La Política se configura como estándar corporativo del Grupo Stratesys y será adoptada o asumida por las sociedades que lo integran conforme a su normativa, estructura de gobierno y proceso interno de aprobación. A estos efectos, se entiende por Grupo Stratesys el conjunto formado por STRATESYS Technology Solutions, S.L. y las sociedades que se encuentren bajo su control directo o indirecto.

2.2 Personas Sujetas

La Política resulta aplicable, en los términos legal o contractualmente procedentes, a:

- Miembros de los órganos de administración y de dirección.
- Personas trabajadoras, cualquiera que sea su modalidad contractual o lugar de prestación de servicios.
- Personal temporal, becarios, personas en formación y colaboradores.
- Profesionales autónomos, agentes y representantes que actúen por cuenta del Grupo.
- Proveedores, contratistas, subcontratistas, socios de negocio y demás terceros cuando así resulte de su contrato, de la normativa aplicable o de la naturaleza de la relación.

Las personas incluidas en este ámbito se denominan conjuntamente Personas Sujetas. Cada una deberá conocer y cumplir las obligaciones que correspondan a sus funciones y nivel de responsabilidad.

3. Principios generales

Legalidad e integridad. Ningún objetivo comercial, económico u operativo justifica el incumplimiento de la ley o de esta Política.

Tolerancia cero. El Grupo rechaza la corrupción, el fraude, el soborno, el blanqueo de capitales y cualquier conducta delictiva.

Responsabilidad individual. Cada Persona Sujeta debe actuar con diligencia, solicitar asesoramiento ante la duda y comunicar los riesgos o incumplimientos de los que tenga conocimiento.

Proporcionalidad. Los controles y las respuestas se adaptarán a la naturaleza, gravedad y probabilidad de los riesgos.

Independencia e imparcialidad. Las funciones de supervisión e investigación actuarán sin injerencias indebidas y gestionarán adecuadamente los conflictos de interés.

Confidencialidad y protección. La información se tratará de forma reservada y se protegerá a las personas informantes frente a represalias en los términos establecidos por la ley.

Respeto a los derechos. Las actuaciones internas respetarán la dignidad, la presunción de inocencia, el derecho de defensa, la privacidad y los demás derechos de las personas afectadas.

Mejora continua. El sistema se revisará ante cambios normativos, organizativos, de actividad o cuando se detecten deficiencias relevantes.

4. Gobernanza y responsabilidades

4.1 Órganos de administración

Los órganos de administración o de gobierno competentes adoptan y promueven el Modelo de Prevención que corresponda, aprueban esta Política, asignan recursos adecuados, designan los órganos o funciones exigidos por la normativa y reciben información periódica sobre su funcionamiento, sin perjuicio de las competencias propias de cada sociedad.

4.2 Comité de Cumplimiento Normativo

El Comité de Cumplimiento Normativo, o la función equivalente designada en cada sociedad, supervisa el funcionamiento y la eficacia del sistema de prevención penal dentro del ámbito que le haya sido atribuido. Actúa con autonomía funcional, acceso suficiente a la información y capacidad para elevar recomendaciones a los órganos competentes.

- Impulsar la evaluación periódica de riesgos y controles.
- Proponer políticas, procedimientos, formación y acciones de mejora.
- Supervisar la ejecución de planes de acción y el tratamiento de deficiencias.
- Informar periódicamente y, cuando proceda, de forma inmediata a los órganos de administración.
- Coordinarse con el Responsable del Sistema respetando la independencia, la confidencialidad y las reglas de acceso a la información.

4.3 Responsable del Sistema Interno de Información

El Responsable del Sistema ejerce las funciones que le atribuya la normativa aplicable y responde de la tramitación diligente de las comunicaciones recibidas a través del Sistema Interno de Información. Desarrollará sus funciones de forma independiente y autónoma, sin recibir instrucciones sobre la gestión de casos concretos.

Separación funcional: El Comité de Cumplimiento Normativo supervisa el modelo de prevención; el Responsable del Sistema gestiona las comunicaciones. La coordinación no permite crear canales paralelos ni acceder indiscriminadamente a la identidad del informante o a información reservada.

4.4 Dirección, mandos y áreas de negocio

La Dirección y los responsables de área deben integrar los controles de cumplimiento en la actividad ordinaria, actuar de manera ejemplar, facilitar los recursos necesarios, responder a las recomendaciones de Cumplimiento y evitar cualquier represalia o interferencia en la comunicación e investigación de posibles incumplimientos.

4.5 Personas Sujetas

Todas las Personas Sujetas deberán cumplir esta Política, participar en la formación que les corresponda, conservar la documentación de forma íntegra, cooperar lealmente con las investigaciones y comunicar las situaciones de riesgo o posibles infracciones por los cauces habilitados.

5. Integración en el Modelo de Prevención

Esta Política se integra en un conjunto más amplio de medidas organizativas y de gestión. En las sociedades sujetas al artículo 31 bis del Código Penal, el Modelo de Prevención deberá incluir, de forma adaptada a su actividad y tamaño:

1. La identificación de las actividades en cuyo ámbito puedan cometerse los delitos que deben ser prevenidos y la evaluación periódica de los riesgos asociados.
2. Protocolos o procedimientos que concreten el proceso de formación de la voluntad, adopción de decisiones y ejecución de estas.
3. Modelos de gestión de recursos financieros adecuados para impedir o dificultar la comisión de delitos.
4. La obligación de informar de posibles riesgos e incumplimientos al órgano o función responsable de vigilar el modelo.
5. Un sistema disciplinario que sancione adecuadamente los incumplimientos, con pleno respeto de la normativa laboral y de los derechos aplicables.
6. La verificación periódica del modelo y su modificación cuando se produzcan infracciones relevantes o cambios en la organización, estructura de control o actividad.

La existencia de esta Política no sustituye la ejecución efectiva de los controles. Las evidencias de aplicación, seguimiento, formación, investigación y mejora deberán conservarse conforme a los procedimientos internos y a la normativa aplicable.

6. Principales áreas de riesgo penal

La evaluación de riesgos determinará los riesgos concretos de cada sociedad y actividad. Sin carácter exhaustivo, el Grupo prestará especial atención a las siguientes áreas:

Corrupción y tráfico de influencias. Sobornos, pagos de facilitación, regalos indebidos, corrupción entre particulares, corrupción de autoridades o funcionarios y utilización de influencias personales para obtener ventajas.

Fraude, estafa y falsedades. Engaño, manipulación documental, facturación falsa, alteración de datos, apropiación indebida, administración desleal o simulación de operaciones.

Hacienda Pública y Seguridad Social. Incumplimientos tributarios o de cotización, obtención indebida de ayudas, subvenciones o beneficios públicos y ocultación o falseamiento de información.

Blanqueo de capitales y financiación ilícita. Utilización, recepción, transferencia u ocultación de fondos o activos de origen ilícito y operaciones carentes de justificación económica razonable.

Insolvencias punibles. Ocultación o disposición irregular de activos, agravación de insolvencias y actuaciones destinadas a frustrar procedimientos ejecutivos o derechos de acreedores.

Información, datos y ciberseguridad. Acceso no autorizado, daños informáticos, revelación de secretos, uso indebido de información confidencial, vulneración de datos personales o alteración de sistemas y evidencias electrónicas.

Propiedad intelectual e industrial. Utilización, reproducción o explotación no autorizada de software, contenidos, marcas, diseños, secretos empresariales u otros activos protegidos.

Mercado, competencia y consumidores. Acuerdos restrictivos, manipulación de licitaciones, publicidad engañosa, revelación de secretos, alteración de precios y prácticas desleales.

Derechos laborales y seguridad. Vulneración grave de derechos de las personas trabajadoras, discriminación, acoso, contratación irregular, incumplimientos de seguridad y salud o empleo de personas sin las autorizaciones exigibles.

Medioambiente. Incumplimientos que puedan provocar daños relevantes al medioambiente o contravenir las autorizaciones y controles aplicables.

Contratación pública y fondos públicos. Obtención indebida de contratos, ayudas o fondos mediante fraude, colusión, falsedad, conflicto de interés o influencia ilícita.

7. Normas esenciales de conducta

7.1 Integridad en los negocios

- Queda prohibido ofrecer, prometer, entregar, solicitar o aceptar ventajas indebidas con la finalidad de influir en una decisión o conseguir un trato de favor.
- Los regalos, invitaciones, viajes, donaciones, patrocinios y atenciones deberán ser lícitos, razonables, transparentes y conformes a las políticas internas y a los límites de aprobación aplicables.
- No se realizarán pagos de facilitación. Las relaciones con autoridades y funcionarios públicos estarán sujetas a un estándar reforzado de control y documentación.
- Los conflictos de interés reales, potenciales o aparentes deberán comunicarse y gestionarse antes de intervenir en la decisión correspondiente.

7.2 Veracidad de la información y registros

- Las cuentas, facturas, gastos, partes de trabajo, registros de proyecto, ofertas y demás documentos deberán reflejar de forma completa y veraz las operaciones realizadas.
- Se prohíbe la creación de fondos no registrados, la doble contabilidad, la ocultación de operaciones, la falsificación documental y la destrucción indebida de evidencias.
- Las aprobaciones y segregaciones de funciones establecidas no podrán eludirse ni fraccionarse artificialmente.

7.3 Protección de activos, información y tecnología

- Los activos, sistemas, credenciales y recursos del Grupo se utilizarán exclusivamente para fines legítimos y autorizados.
- La información confidencial, los secretos empresariales, los datos personales y la propiedad intelectual propia o de terceros deberán protegerse durante y después de la relación profesional.
- No se instalará, copiará, desarrollará o utilizará software o contenido sin las licencias, autorizaciones y controles requeridos.
- Todo incidente de seguridad, pérdida de información o acceso indebido deberá notificarse inmediatamente por los cauces establecidos.

7.4 Personas, trabajo y respeto

- El Grupo no tolera la discriminación, el acoso, la violencia, la explotación, el trabajo forzoso ni cualquier vulneración de la dignidad o de los derechos fundamentales.
- Las obligaciones laborales, de Seguridad Social, igualdad, inmigración, prevención de riesgos y seguridad y salud se cumplirán en todas las actividades.
- Ninguna persona sufrirá represalias por solicitar asesoramiento, rechazar una conducta ilícita o comunicar de forma protegida una posible infracción.

7.5 Cumplimiento fiscal, financiero y de competencia

- Las obligaciones fiscales, contables, de Seguridad Social y de control financiero se cumplirán de forma exacta, completa y dentro de plazo.
- Se comprobará la identidad, legitimidad y razonabilidad económica de las operaciones y contrapartes cuando lo exijan el riesgo o los procedimientos internos.
- Las Personas Sujetas actuarán de forma independiente frente a competidores y evitarán acuerdos o intercambios de información que puedan restringir indebidamente la competencia.

8. Relaciones con terceros

El Grupo espera que los terceros con los que se relaciona mantengan estándares de integridad compatibles con esta Política. La selección, contratación y supervisión se realizará con criterios objetivos, trazables y proporcionales al riesgo.

- Realizar comprobaciones de integridad y solvencia cuando lo exijan el riesgo, la normativa o los procedimientos internos.
- Definir por escrito el alcance, contraprestación, responsabilidades y obligaciones de cumplimiento.
- Incluir cláusulas de cumplimiento, auditoría, información y terminación cuando resulten proporcionadas.
- Evitar pagos en efectivo, cuentas de terceros, jurisdicciones injustificadas, comisiones desproporcionadas o servicios insuficientemente descritos.
- Supervisar la prestación y documentar las incidencias, alertas y medidas correctoras.

Cada tercero responderá de sus propias obligaciones. Lo anterior no excluirá ni limitará las responsabilidades que legalmente correspondan a las sociedades del Grupo.

9. Formación, información y asesoramiento

El Grupo desarrollará acciones de comunicación y formación periódica adaptadas a las funciones, exposición al riesgo y responsabilidad de las Personas Sujetas. La participación podrá ser obligatoria y quedará documentada.

- Formación de incorporación y actualizaciones periódicas.
- Formación reforzada para áreas de mayor riesgo, dirección y órganos de gobierno.
- Comunicaciones sobre cambios normativos, incidentes, controles y lecciones aprendidas.
- Canales de consulta accesibles para resolver dudas antes de actuar.

Ante una duda, deberá suspenderse la actuación cuando sea razonablemente posible y solicitarse asesoramiento a Legal, Cumplimiento Normativo o a la función especializada que corresponda. La consulta preventiva se considera una conducta responsable y no generará consecuencias negativas.

10. Sistema Interno de Información – Canal de Denuncias

El Grupo dispone de un Sistema Interno de Información – Canal de Denuncias que permite comunicar de forma segura y confidencial posibles infracciones, incumplimientos o irregularidades conocidas en un contexto laboral o profesional relacionado con el Grupo.

Las comunicaciones podrán presentarse a través del Portal de Denuncias del Grupo Stratesys, gestionado mediante una plataforma externa que permite su presentación y seguimiento seguro. El Canal admite comunicaciones anónimas.

[ACCEDER AL PORTAL DE DENUNCIAS – CENTINELA]

También podrán emplearse los restantes medios previstos en los procedimientos internos y en la normativa aplicable. La utilización del Canal interno no es obligatoria ni impide acudir directamente a las autoridades o canales externos competentes.

10.1 Garantías

- Confidencialidad de la identidad del informante, de las personas afectadas y de los terceros mencionados, con las excepciones previstas legalmente.
- Posibilidad de realizar comunicaciones anónimas.
- Prohibición de represalias, incluidas las amenazas y tentativas, cuando concurren las condiciones legales de protección.
- Gestión independiente, imparcial y diligente de las comunicaciones.
- Respeto de los derechos de la persona afectada y protección de los datos personales.

10.2 Uso responsable

La protección no exige aportar pruebas concluyentes, pero sí motivos razonables para considerar que la información era veraz en el momento de comunicarla y que se encontraba dentro del ámbito protegido. Los errores de buena fe no serán sancionados. Las comunicaciones deliberadamente falsas o realizadas con abuso podrán dar lugar a las medidas que procedan.

El Canal no es un servicio de emergencia ni está destinado a consultas o reclamaciones comerciales. Estas cuestiones deberán dirigirse a los servicios de emergencia o a los canales ordinarios de contacto y atención, según corresponda.

10.3 Documentación aplicable

[Política y Protocolo del Sistema Interno de Información – España]

[Información específica aplicable a Portugal]

11. Investigación y respuesta

Las comunicaciones se tramitarán conforme al procedimiento aplicable en cada jurisdicción. La recepción de una comunicación no implica por sí misma que los hechos sean ciertos ni que se haya producido una infracción.

- Análisis preliminar de competencia, alcance, suficiencia y posibles conflictos de interés.
- Admisión, inadmisión o remisión al canal o función competente conforme al procedimiento.
- Investigación objetiva, proporcionada, documentada y limitada a la información necesaria.
- Respeto de la presunción de inocencia, el derecho de defensa, la confidencialidad y los derechos de las personas afectadas.
- Conclusión motivada y adopción de medidas correctoras, disciplinarias, contractuales o legales cuando proceda.

Cuando los hechos pudieran ser indiciariamente constitutivos de delito, se actuará conforme a la normativa aplicable, incluida la remisión inmediata al Ministerio Fiscal y, cuando afecten a los intereses financieros de la Unión Europea, a la Fiscalía Europea, en los supuestos legalmente previstos.

Las áreas y Personas Sujetas deberán colaborar de forma veraz y preservar la documentación relevante. Queda prohibido destruir, alterar u ocultar evidencias o interferir en la investigación.

12. Consecuencias del incumplimiento

El incumplimiento de esta Política podrá dar lugar a la adopción de las medidas disciplinarias, contractuales o legales que correspondan, atendiendo a la naturaleza y gravedad de los hechos, la responsabilidad de la persona, la reiteración, el daño causado y las demás circunstancias relevantes.

Las medidas se aplicarán con respeto de la legislación laboral, los convenios colectivos, los contratos, los procedimientos internos y los derechos de audiencia y defensa. En el caso de terceros, podrán incluir planes correctores, suspensión, auditoría, reclamación de daños o terminación de la relación cuando resulte legal y contractualmente procedente.

Las consecuencias internas se entenderán sin perjuicio de las responsabilidades administrativas, civiles o penales que pudieran existir.

13. Protección de datos y conservación

Los datos personales tratados en aplicación de esta Política se gestionarán conforme al Reglamento (UE) 2016/679, la Ley Orgánica 3/2018, la Ley 2/2023 y la normativa local que resulte aplicable. El tratamiento no dependerá necesariamente del consentimiento, sino de las bases jurídicas previstas por la normativa para el cumplimiento de obligaciones legales, la investigación y prevención de ilícitos y la protección de los derechos e intereses legítimos correspondientes.

El acceso a los datos se limitará a las personas autorizadas y a la información necesaria para sus funciones. Se aplicarán medidas de seguridad, trazabilidad, confidencialidad y conservación adecuadas. Los plazos de conservación del Sistema Interno de Información y de los expedientes de investigación serán los establecidos en el procedimiento y en la normativa aplicable.

La información detallada sobre el tratamiento de datos personales estará disponible en el Portal de Denuncias y en las políticas de privacidad aplicables.

14. Seguimiento, revisión y entrada en vigor

14.1 Seguimiento

El Comité de Cumplimiento Normativo o la función equivalente supervisará el grado de implantación de esta Política mediante indicadores, revisiones de controles, seguimiento de planes de acción, resultados de formación, auditorías e información agregada sobre incidentes, respetando en todo caso la confidencialidad del Sistema Interno de Información.

14.2 Revisión

La Política se revisará periódicamente y, en particular, cuando:

- Se produzcan cambios normativos relevantes.
- Cambien sustancialmente la actividad, estructura, mercados, servicios o modelo organizativo del Grupo.
- Se detecten infracciones relevantes, deficiencias de control o nuevas tipologías de riesgo.
- Las evaluaciones, auditorías o investigaciones recomienden su actualización.

14.3 Aprobación y adhesión

La Política será aprobada por el órgano competente de cada sociedad a la que resulte aplicable. Las sociedades del Grupo podrán adherirse a esta versión corporativa o aprobar las adaptaciones locales necesarias, sin reducir las garantías mínimas aquí establecidas.

14.4 Entrada en vigor y difusión

La Política entrará en vigor desde su aprobación y publicación interna o externa, según corresponda, y permanecerá accesible para las Personas Sujetas. Sustituye a las versiones anteriores en el ámbito de la sociedad que la adopte.

ANEXO. Documentos relacionados

Esta Política se complementa, entre otros, con los siguientes documentos corporativos:

- Código de Conducta del Grupo Stratesys.
- Mapa de riesgos penales y controles aplicables a las sociedades del Grupo.
- Política y Protocolo del Sistema Interno de Información – España.
- Información específica aplicable a Portugal.
- Políticas y procedimientos anticorrupción, de regalos, conflictos de interés y relaciones con terceros que resulten aplicables.
- Políticas de privacidad, seguridad de la información, uso de sistemas y conservación documental.
- Régimen disciplinario y procedimientos laborales aplicables.

Interpretación: En caso de contradicción, se aplicará la norma imperativa correspondiente y, entre documentos internos del mismo rango, la disposición más específica para la materia y jurisdicción de que se trate.