



**POLÍTICA
ESTRATEGIA DEL
SISTEMA INTERNO
DE INFORMACIÓN**

Índice

1. DEFINICIONES	1
2. FINALIDAD	6
3. ALCANCE	7
4. SISTEMA INTERNO DE COMUNICACIÓN	8
5. PARÁMETROS DE PROTECCIÓN	10
4.1 COLECTIVO SUSCEPTIBLE DE PROTECCIÓN	10
4.2 CONDICIONES DE LA PROTECCIÓN	10
4.3 MEDIDAS DE PROTECCIÓN AL INFORMANTE Y TERCEROS RELACIONADOS	10
4.4 MEDIDAS DE PROTECCIÓN A LAS PERSONAS AFECTADAS POR LA COMUNICACIÓN	12
4.5 ACTIVACIÓN DE LA PROTECCIÓN	12
6. FORMACIÓN	14
7. CANALES EXTERNOS DE INFORMACIÓN	15
8. CONSECUENCIAS DEL INCUMPLIMIENTO	16
9. CONOCIMIENTO Y ENTRADA EN VIGOR	17
ANEXOS	
ANEXO 1.	18

1. DEFINICIONES

Se relacionan a continuación las definiciones de aquellos conceptos que se utilizarán de manera frecuente en el presente documento.

Definiciones relacionadas con la estructura organizativa de STEF:

- **STEF / la Organización:** incluye a las entidades que se encuentran adheridas y a las que les resultare aplicación el Modelo de Prevención de Delitos de Grupo STEF en España.
- **Órgano de Control (OC):** órgano interno de cumplimiento penal de STEF, dotado de poderes autónomos de iniciativa y control, al que se le confía, entre otros cometidos, la responsabilidad de supervisar el funcionamiento y observancia del Modelo de Prevención de Delitos de STEF. La existencia del OC responde a las exigencias establecidas en la normativa penal española (artículo 31 bis del Código penal español) en cuanto a la supervisión del Sistema.
- **Consejo de Administración:** órgano de administración de STEF, en la medida que tiene asignadas la responsabilidad y autoridad fundamental de las actividades, la gobernabilidad y las políticas de la Organización.
- **Miembros de la Organización:** los integrantes del Consejo de Administración, la Alta Dirección, directivos, empleados, trabajadores o empleados temporales o bajo convenio de colaboración y, voluntarios de la Organización y el resto de las personas bajo subordinación jerárquica de cualquiera de los anteriores.
- **Alta Dirección:** personas encargadas de dirigir y controlar STEF al más alto nivel. Actualmente, la Alta Dirección de STEF está compuesta por las Direcciones Operativas de Unidad de Negocio, así como las Direcciones Funcionales a saber, la Dirección de Control de Gestión Operativa, la Dirección de Financiero y Compras, la Dirección Grandes Cuentas y

Marketing, la Dirección de Operaciones, la Dirección de Recursos Humanos, la Dirección de Sistemas Informáticos y la Dirección Técnica

- **Socios de negocio:** cualquier persona física o jurídica, salvo los Miembros de la Organización, con quien la Organización mantiene o prevé establecer algún tipo de relación de negocio. A modo enunciativo, pero no limitativo, se incluyen clientes, proveedores, intermediarios como los colaboradores externos o captadores de clientes, inversores, asesores externos, joint-ventures y personas físicas o jurídicas contratadas por STEF para la entrega de bienes o para la prestación de servicios.
- **Tercero:** persona física o jurídica ajena a la Organización u órgano independiente con el que se relaciona la Organización.
- **Modelo de Prevención de Delitos:** sistema de organización que permite prevenir, detectar y gestionar los riesgos de comisión de delitos atribuibles a la persona jurídica en España conforme a la legislación vigente, así como aquellos que pueden afectar de manera significativa a los empleados, responsables y administradores de la Organización.

Definiciones relacionadas con el Sistema interno de información de STEF:

- **Canal de denuncias de STEF:** sistema interno de información, a los efectos 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 y en cumplimiento de las obligaciones y requisitos previstos en la misma, y que permite la interposición de comunicaciones (denuncias y consultas).
- **Responsable del Sistema interno de información:** órgano designado por el Consejo de Administración, encargada de la gestión del Sistema interno de información de STEF de manera independiente y autónoma. STEF ha notificado a la Autoridad Independiente de Protección al Informante A.A.I. la identidad del Responsable del Sistema.

En STEF la figura de Responsable del Sistema recae sobre el Órgano de Control de la Organización. Al tratarse el Responsable del Sistema de un órgano colegiado, este ha delegado en uno de sus miembros las facultades de gestión del Sistema y de tramitación de expedientes de investigación.

En cualquier caso, STEF ha optado por una gestión mixta del Canal de denuncias, recibiendo el Responsable del Sistema apoyo externo por parte del despacho de abogados ECIJA LEGAL.

La existencia del 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.

- **Denuncia:** comunicación relativa a una infracción (comportamiento activo u omisivo) de la normativa aplicable a STEF, especialmente, se entenderán infracciones a comunicar a través del Sistema interno de información las siguientes:
 - Infracciones del Derecho de la Unión Europea relativas, entre otros, a los siguientes ámbitos: contratación pública, sector financiero, prevención del blanqueo de capitales o financiación del terrorismo, seguridad de los productos y conformidad, seguridad del transporte, protección del medio ambiente, protección frente a las radiaciones y seguridad nuclear, seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales, salud pública, protección de los consumidores, protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información, intereses financieros de la Unión y mercado interior.
 - Infracciones penales o administrativas graves o muy graves.
 - Conductas contradictorias con los valores y principios recogidos en el Código Ético de STEF.

- Conductas no conformes con las políticas y procedimientos internos de STEF.
 - Indicios de supuestos de hecho en materia de acoso laboral y/o sexual.
 - Conductas contrarias a los compromisos y obligaciones de STEF con proveedores y otros terceros.
 - Alerta de conflictos de interés, contrarios a la normativa, dónde exista un riesgo de conflicto personal o de grupo en relación al mejor interés corporativo de STEF.
 - Otras conductas o comportamientos susceptibles de suponer un riesgo relevante para la responsabilidad o la reputación de STEF.
- **Consulta:** comunicación por la que se solicita una aclaración, respuesta o criterio sobre el alcance, interpretación o incumplimiento de la normativa aplicable a STEF.
 - **Comunicaciones:** Denuncias y Consultas, conjuntamente.
 - **Informante:** persona física o jurídica que interpone una Consulta o Denuncia. La figura del Informante comprende, no solo a los empleados públicos o trabajadores por cuenta ajena, sino también a todos aquellos trabajadores autónomos, los accionistas, partícipes y miembros del órgano de administración, dirección o supervisión de la empresa, las personas que trabajen para o bajo la supervisión de socios de negocio, voluntarios, becarios y trabajadores en periodo de formación, así como las personas cuya relación laboral o estatutaria esté finalizada o no haya comenzado.
 - **Terceros relacionados:** Esta figura incluye aquellas personas de la organización que asistan al informante en el proceso, así como a las personas relacionadas que puedan sufrir represalias, tales como compañeros de trabajo o familiares.

- **Persona afectada por la comunicación:** persona o personas físicas o jurídicas a las que se le imputa una Denuncia sobre una presunta infracción.

2. FINALIDAD

La presente Política desarrolla los principios que revisten al Canal de denuncias de STEF, como cauce preferente para informar sobre las acciones u omisiones, que serán en todo caso tratadas de manera efectiva por parte de la Organización.

Como muestra de su compromiso con la cultura ética y de cumplimiento, el Consejo de Administración-previa consulta con la representación legal de los trabajadores, ha implantado un Sistema interno de información en el seno de la Organización y ha aprobado la presente Política, con la finalidad de establecer un estándar de protección a los Informantes.

La presente Política se ha desarrollado procurando su alineación con la siguiente normativa de aplicación:

- **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.
- **Directiva (UE) 2019/1937** del Parlamento Europeo y del Consejo de 23 de octubre de 2019.
- **LDE**: Ley 1/2019, de 20 de febrero, de Secretos Empresariales.
- **RGPD**: Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
- **LOPDGDD**: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- **TFUE**: Tratado de Funcionamiento de la Unión Europea.
- **Norma UNE 19601:2017, sobre sistemas de gestión de Compliance penal**
- **Norma ISO 37002:2021, sobre sistemas de gestión de denuncias.**

3. ALCANCE

La presente política es de obligado cumplimiento y de aplicación para todas las entidades que componen la Organización de acuerdo con la definición del apartado 1 de la misma. Y, por tanto, para todos los Miembros de la Organización, independientemente del cargo que ocupen o de su ubicación geográfica.

Las diferentes medidas de protección previstas en la presente política se ejercerán, según correspondan, sobre todos los Informantes, Terceros relacionados y Personas afectadas por la comunicación.

4. SISTEMA INTERNO DE COMUNICACIÓN

STEF se ha dotado de un mecanismo de reporte y comunicación interna. Por ello, eventuales Consultas y Denuncias podrán cursarse, tanto de forma anónima como nominal, a través del software externo (Global Suite) licenciado por la compañía AUDISEC y que garantiza los principios y garantías de Informante, Terceros relacionados y personas afectadas por la comunicación, al que se puede acceder a través del siguiente enlace:

[GlobalSUITE Whistleblower Channel \(globalsuitesolutions.com\)](https://globalsuite.com/whistleblower-channel)

Las comunicaciones recibidas pueden referirse a hechos conocidos en el ámbito de una relación laboral o profesional (i) todavía en vigor, (ii) ya finalizada o (iii) incluso no iniciada (por ejemplo, si se refiere a infracciones relativas a procesos de selección o de negociación precontractual).

Toda Consulta o Denuncia terminará siendo gestionada por el Responsable del Sistema, en los términos descritos en el **Procedimiento y Guía de uso del Canal de denuncias**.

No obstante, a los efectos de garantizar una mayor independencia, STEF ha contratado los servicios de un gestor externo encargado de la recepción de las Comunicaciones, así como de aplicar los filtros correspondientes para la prevención de conflictos de intereses, optimizando los niveles de autonomía, independencia y confidencialidad. Actualmente las citadas funciones de gestión externa del Canal de Denuncias se realizan por parte del despacho ÉCIJA.

En cualquier caso, STEF velará porque los canales de comunicación constituyan un medio seguro, cumpliendo con la normativa de protección de datos personales aplicable y garantizando los derechos de los Informantes, Terceros relacionados y Personas afectadas por la Comunicación, así como su confidencialidad. Del mismo modo, STEF velará porque no se adopten

represalias contra ellos cuando utilicen los canales de comunicación de buena fe.

5. PARÁMETROS DE PROTECCIÓN

4.1 COLECTIVO SUSCEPTIBLE DE PROTECCIÓN

La Organización 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 incumplimientos de los que hayan tenido conocimiento.

Asimismo, la Organización extenderá la protección a las Personas afectadas por la Comunicación.

4.2 CONDICIONES DE LA PROTECCIÓN

Se considera Informante de buena fe aquel que tengan motivos razonables para pensar que la información referida es veraz en el momento de la Comunicación, aun cuando no aporten pruebas concluyentes, y que la citada información entra dentro del ámbito de aplicación de esta ley.

Quedan expresamente excluidas del Canal de denuncias de STEF las informaciones contenidas en Comunicaciones que hayan sido previamente inadmitidas por algún canal interno de información, así como aquellas cuyos hechos no se encuentren comprendidos en la definición de Denuncia o Consulta prevista en el apartado 1 de la presente Política.

4.3 MEDIDAS DE PROTECCIÓN AL INFORMANTE Y TERCEROS RELACIONADOS

La Organización /STEF es responsable de garantizar la protección a los Informantes y Terceros relacionados. Por su parte, el Órgano de Control, como Responsable del Sistema, es responsable de asegurar que dichas medidas de protección se llevan a cabo de forma efectiva en la Organización.

PROHIBICIÓN DE REPRESALIAS

Todo Miembro de la Organización 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 cualesquier acto u omisión que estén prohibidos por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, solo por su condición de Informantes o Terceros relacionados, o por haber realizado una revelación pública.

Se adjunta como **Anexo 1** un listado ejemplificativo, no limitativo, de acciones o actos encuadrables en la definición de represalia.

Si STEF tiene conocimiento de que se está llevando o se ha llevado a cabo una represalia, esta 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. Por ejemplo:

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

CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES

La Organización 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.

STEF se compromete a no recopilar datos personales cuya pertinencia no resulte manifiesta para tratar una información específica o, si se recopilan por accidente, se eliminarán sin dilación indebida.

4.4 MEDIDAS DE PROTECCIÓN A LAS PERSONAS AFECTADAS POR LA COMUNICACIÓN

Las principales medidas de protección que se implementarán sobre las Personas afectadas por la Comunicación son las siguientes:

- a) Garantizar el derecho a la presunción de inocencia;
- b) Proteger su identidad (en la medida de lo posible);
- c) Realizar las investigaciones preservando la confidencialidad, en la medida de lo posible, y garantizando que estos no estén expuestos a daños reputacionales (la información se compartirá sobre una base estrictamente necesaria);
- d) Garantizar el debido proceso, incluida una investigación oportuna, justa, imparcial y confidencial, así como permitirle el acceso al expediente, dentro de los límites oportunos.
- e) Brindar apoyo durante todo el proceso, incluida la comunicación regular y garantizar su derecho de defensa;
- f) Si no se encontró evidencia de irregularidades, se pueden considerar medidas correctivas adicionales, p. ej. reputación, situación financiera, laboral.

4.5 ACTIVACIÓN DE LA PROTECCIÓN

Las medidas de protección y el apoyo al Informante, los Terceros relacionados y las Personas afectadas por la Comunicación se activarán y darán comienzo

tan pronto como se reciba una Consulta o una Denuncia, y continuará durante e incluso después -cuando sea preciso- de la conclusión del proceso de investigación o gestión de la Consulta o Denuncia.

6. FORMACIÓN

Todas las personas susceptibles de gestionar Consultas y Comunicaciones de acuerdo con la presente Política recibirán formación en la materia, relacionada con el procedimiento a seguir y las garantías y medidas de protección a ofrecer a Informantes, Terceros relacionados y Personas afectadas por la Comunicación.

Cualquier quebranto de lo dispuesto en la presente Política por parte de las personas que gestionan Comunicaciones será tipificado como infracción muy grave.

Se entienden como personas susceptibles de gestionar Consultas y Denuncias no solo los miembros del Órgano de Control, como Responsable del Sistema, sino también aquellos directivos cuyas funciones de gestión de equipo puedan incentivar entre sus miembros la eventual comunicación verbal, por tratarse de una figura de superior jerárquico.

7. CANALES EXTERNOS DE INFORMACIÓN

Adicionalmente al Canal de denuncias de STEF, se pone en conocimiento de todos los eventuales Informantes la existencia de canales externos de información, entre los que se encuentran:

- Canal externo de información de la Autoridad Independiente de Protección al Informante A.A.I.: [pendiente de creación]
- Canal externo de comunicaciones de la Dirección de Competencia de la CNMC: <https://sede.cnmc.gob.es/tramites/competencia/denuncia-de-conducta-prohibida>
- Banco de España: <https://clientebancario.bde.es/pcb/es/menu-horizontal/podemosayudarte/consultasreclama/comorealizarrecl/>
- AEPD: <https://www.aepd.es/es/preguntas-frecuentes/13-reclamaciones-ante-aepd-y-ante-otros-organismos-competentes/FAQ-1301-como-puedo-interponer-una-reclamacion-si-han-vulnerado-mis-datos-de-caracter-personal>
- Hacienda: <https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/paginas/comunicacionsnca.aspx>
- CNMV: <https://www.cnmv.es/Portal/Whistleblowing/Formulario.aspx>
- [...]

8. 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 grave del mismo, o de cualquier otro elemento del Modelo de Prevención de Delitos, este podrá y deberá ser puesto en conocimiento del Órgano de Control a través del Canal de denuncias.

Cuando se investigue y confirme la contravención de lo indicado por estos textos, se adoptarán las medidas disciplinarias (en el ámbito laboral) o contractuales (en las relaciones mercantiles con Socios de Negocio) que considere proporcionales al riesgo o daños ocasionados.

Las medidas que se adopten desde una perspectiva laboral serán respetuosas con la normativa aplicable, sin que por ello pierdan contundencia o proporcionalidad con la gravedad de los hechos de los que traigan causa, informando si procede a la Representación Legal de los Trabajadores.

En el caso que se confirme que la actuación de algún Miembro de la Organización pudiera ser constitutiva de un ilícito penal por el que puede ser investigada la persona jurídica, tal circunstancia será puesta de manifiesto a las Autoridades Públicas competentes para su conocimiento y persecución. Tal comunicación se acompañará con las evidencias y/o indicios que se hayan podido recopilar al respecto.

9. CONOCIMIENTO Y ENTRADA EN VIGOR

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://channel.globalsuitesolutions.com/stef>

ANEXOS

ANEXO 1.

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 denunciante,
- Pérdida financiera,
- Anulación o denegación de una licencia o permiso.