POLÍTICA DEL SISTEMA INTERNO DE INFORMACIÓN

CONTROL DE VERSIONES			
VERSIÓN	**FECHA**	**RESPONSABLE**	**OBSERVACIONES**
1.0	25/09/2019	Compliance penal	Delimitación y contenido del Reglamento del Canal de Denuncias de acuerdo con el Código Penal
2.0	27/02/2023	Compliance penal	Adaptación a 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.
2.1	30/06/2023	Compliance penal	Revisión, actualización e inclusión de anexos
2.2	15/01/2024	Compliance Penal	Revisión y corrección en materia de protección de datos.
2.3	08/03/2024	Compliance penal	Revisión e inclusión de introducción y delitos del anexo I de la Directiva Europea 2019/1937
2.4	18/11/2024	Compliance penal	Revisión y corrección de errores
	19/12/2025	Compliance penal	Revisión y modificación de la finalidad

ÍNDICE

1.- INTRODUCCIÓN 4
2.- FINALIDAD 4
3.-ALCANCE 5
¿Qué conductas se pueden denunciar a través del sistema interno de información? 5
¿Quién está legitimado para informar a través del SII? 5
4. SISTEMA INTERNO DE INFORMACIÓN 6
4.1- Principios básicos del sistema interno de información 6
4.2 Canal interno de información 7
4.3 Procedimiento del SII 8
4.4 Canales externos 8
5.- RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN (RSII) 8
6.- MEDIDAS DE PROTECCIÓN Y GARANTÍAS 9
6.1 Condiciones de protección 9
6.2 Exclusiones de protección 9
6.3 Extensión de la protección 9
6.4 Prohibición de represalias 9
6.5 Medidas de apoyo 10
6.6 Medidas de protección 10
6.7 Medidas de protección de la persona afectada por una comunicación 10
7.- LIBRO-REGISTRO DE INFORMACIONES 11
8.- PROTECCIÓN DE DATOS PERSONALES 11
8.1 Régimen jurídico del tratamiento de datos personales 11
8.2 Límites del tratamiento 11
8.3 Licitud del tratamiento 12
8.4 Información a interesados 12
8.5 Preservación de datos 12
8.6 Acceso a datos en el SII 12
8.7 Identidad del informante 12
ANEXO I.- PROCEDIMIENTO DE GESTIÓN DEL SII 12

1.- PROCEDIMIENTO DE COMUNICACIÓN DE ACTUACIONES IRREGULARES. 12
1.1 Identificación de una irregularidad. 12
1.2 Comunicación/Recepción de la comunicación. 13
1.3 Requisitos mínimos de la comunicación. 14
1.4 Anonimato 14
2.- PROCEDIMIENTO DE GESTIÓN COMUNICACIONES 15
2.1 Recepción de la información 15
2.2 Registro y clasificación de la comunicación 15
2.3 Trámite de admisión 15
2.4 Desarrollo de la investigación 16
2.5 Procedimiento de instrucción 17
2.6 Resolución de la comunicación 18
2.7 Terminación de las actuaciones 18
3.- ELABORACIÓN DE INFORME ANUAL 19
ANEXO II.- FORMULARIO DE COMUNICACIÓN DE INFORMACIONES RELATIVAS A 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. 20
ANEXO III PROTOCOLO DE CONFIDENCIALIDAD 22
1. OBJETIVO 22
2. RESPONSABILIDAD DEL PERSONAL 22
3. PROCEDIMIENTO EN CASO DE RECEPCIÓN DE COMUNICACIONES POR CANALES NO OFICIALES 22
4. INFORMACIÓN Y SENSIBILIZACIÓN 23

1.- INTRODUCCIÓN

La presente política se aprueba para dar cumplimiento a 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, incorpora al Derecho español la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019.

Esta normativa regula, entre otras cosas, el Sistema interno de información y la protección adecuada frente a las represalias que puedan sufrir las personas físicas que informen sobre alguna de las acciones u omisiones del Derecho de la Unión Europea, derecho penal, normativa laboral, etc.

En este sentido, desde el año 2019, Grupo Fedola ya había implementado un canal de información, denominado canal de denuncias, como complemento a su Código Ético, para que cualquier persona trabajadora dispusiese de una vía de comunicación para informar de actuaciones no conformes con las leyes, reglamentos o políticas internas, susceptibles de ser motivadoras de responsabilidad penal por parte de la empresa. Esta vía estaba ya disponible en el sitio de internet, www.grupofedola.com. En cumplimiento del artículo 7 de la Ley 2/2023, este canal de denuncias pasa a ser parte del Sistema interno de información.

Por todo lo anterior, el Consejo de Administración de Grupo Fedola implanta el sistema interno de información común para las empresas que conforman el Grupo (en adelante, SII). Este sistema se podrá utilizar de forma alternativa a otros canales externos si así lo desea el informante, siendo el canal interno de información el cauce preferente para informar de cualquier conducta que pueda resultar ilícita o irregular, dentro del ámbito objetivo de esta política.

2.- FINALIDAD

La finalidad de la presente política es determinar los principios, normas, derechos y obligaciones del sistema interno de información del Grupo Fedola.

De conformidad con lo dispuesto en el artículo 11 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, se aprueba el presente sistema interno de información para todo el Grupo Fedola. Las mercantiles independientes que comprenden el Grupo Fedola son las siguientes:

GRUPO FEDOLA, S.L.

PREFABRICADOS TEIDE, S.L.

FERRETERIA HERMANOS LÓPEZ ARVELO, S.L.U.

FEDOLA, S.L.U.

BROKER FEDOLA CORREDURÍA DE SEGUROS, S.L.U.

PRICEMESA, S.L.U.

GF-TIC, S.L.U

CAMULSE, S.L.U.

OFISABEL, S.L.U

MASQUECARPAS, S.L.U

AGRO INNOVACIÓN FEDOLA, S.L.U.

GF HOTELES, integrado por:

EXPLOTACIONES SANTONEL, S.L.

FELAHOTEL, S.L.

COSTA ADEJE GRAN HOTEL, S.L.

ISABEL FAMILY HOTEL, S.L.U.

NOELIA PLAYA, S.L.U.

3.-ALCANCE

¿Qué conductas se pueden denunciar a través del sistema interno de información?

a) infracciones del Derecho de la Unión Europea siempre que entren dentro del ámbito de aplicación de los actos de la UE enumerados en el anexo de la Directiva 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019 y que afecten a los intereses financieros de la UE o incidan en el mercado interior.

b) En el ámbito del ordenamiento jurídico español, las infracciones penales, las infracciones administrativas graves y muy graves y las infracciones del Derecho laboral en materia de seguridad y salud en el trabajo.

Las comunicaciones recibidas que se encuentren fuera del ámbito establecido en el artículo 2 de la Ley 2/2023, éstas y sus remitentes quedarán fuera del ámbito de protección dispensado por la misma (art. 7.4).

¿Quién está legitimado para informar a través del SII?

a) las personas que tengan la condición de trabajadores por cuenta ajena de Grupo Fedola;

b) los autónomos;

c) los accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa, incluidos los miembros no ejecutivos;

d) cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

e) aquellos que hayan tenido una relación laboral o estatutaria ya finalizada con Grupo Fedola, voluntarios, becarios, trabajadores en periodos de formación con independencia de que perciban o no una remuneración, así como a aquellos cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.

4. SISTEMA INTERNO DE INFORMACIÓN

El SII de Grupo Fedola que se refiere la presente política es el cauce preferente para informar sobre las acciones u omisiones previstas en el apartado 3 anterior.

El SII se compone, principalmente, del canal de comunicación habilitado para la recepción de las comunicaciones previstas en el ámbito de aplicación, del RSII y del procedimiento que deberá seguirse para la tramitación de las referidas comunicaciones, denominado *"ANEXO I.- Procedimiento del sistema interno de información".*

4.1- Principios básicos del sistema interno de información

El Consejo de Administración de Grupo Fedola establece los principios y reglas para implantar canales de denuncia y gestionar procesos de investigación interna, destacando:

- Accesibilidad: Permite a todas las personas referidas en el apartado 3 de esta política comunicar información sobre las infracciones previstas en dicho apartado, por escrito o verbalmente, pudiendo hacerlo de forma anónima.

- Integración: El canal interno de información establecido en Grupo Fedola está integrado en el SII.

- Seguridad confidencialidad y respeto a la normativa sobre protección de datos: El SII 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 los derechos a la intimidad, la privacidad, al honor , a la defensa y a la presunción de inocencia de las personas involucradas en el proceso de investigación iniciado como consecuencia de la recepción de una comunicación realizada a través del SII, y a la protección de datos, impidiendo el acceso a personal no autorizado.

La identidad del informante, en caso de ser conocida, así como la de los terceros mencionados en la comunicación, sólo podrá ser comunicada a la autoridad judicial, al Ministerio Fiscal o a la Autoridad Administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora, previo traslado al informante o al tercero afectado, siempre que dicha circunstancia no comprometa la investigación o el procedimiento judicial en curso.

- Diligencia, agilidad y efectividad: Las actuaciones dirigidas a la comprobación y esclarecimiento de los hechos recogidos en las comunicaciones recibidas deberán llevarse a cabo con la mayor diligencia, agilidad y efectividad posibles, en atención a la complejidad de los hechos, con el objetivo de que Grupo Fedola sea la primera en conocer la posible irregularidad, y atendiendo, en todo caso, a lo establecido en el procedimiento de gestión del SII.

- Proporcionalidad, objetividad y respeto a las garantías de los intervinientes: las actuaciones desarrolladas en el marco del SII se desarrollarán conforme a criterios de proporcionalidad y objetividad, con el máximo respeto a la legalidad vigente, reconociéndose los derechos que asisten a todas las partes intervinientes y observando las garantías expresamente previstas en el procedimiento de gestión del SII para las personas intervinientes, estando expresamente prohibido cualquier acto constitutivo de represalia contra los informantes.

La persona afectada por la comunicación tiene derecho a ser informada de los hechos que se le atribuyen y a ser oída en cualquier momento. Una vez informada, podrá solicitar el examen de la información y documentación obrante en el expediente a que haya dado lugar la tramitación de la comunicación, si bien deberán adoptarse las medidas necesarias para asegurar que no se revele ningún tipo de información que permita conocer la identidad del informante.

- Buena fe: constituye requisito indispensable para la protección del informante que actúe de buena fe y con conciencia honesta de que se han producido o pueden producirse hechos graves perjudiciales. Dicho principio se contrapone a actuaciones como la remisión de informaciones falsas o tergiversadas, así como las que se han obtenido de manera ilícita.

- Publicidad: la información necesaria para que los informantes puedan hacer uso del canal interno de Grupo Fedola se proporciona de manera clara y fácilmente accesible, estando recogida en esta política, que puede ser consultada en la página web de todas las empresas que conforman Grupo Fedola, y más concretamente a través de la siguiente dirección: https://grupofedola.com/inicio/canal-denuncias/

4.2 Canal interno de información

El canal interno de información, integrado en el SII, permite comunicar infracciones del artículo 2 de la Ley 2/2023 de forma escrita (correo postal o medios electrónicos) o verbal (teléfono, mensajería de voz o reunión presencial, esta última en un plazo máximo de 7 días a solicitud del informante). En el Sistema Interno de Información se integra por el Canal Denuncia.

Las comunicaciones verbales serán documentadas mediante transcripciones exactas, que el informante podrá revisar, rectificar y aceptar. Se informará al informante sobre el tratamiento de sus datos personales según el Reglamento (UE) 2016/679 y los canales externos disponibles para comunicar a autoridades competentes o instituciones europeas.

Es posible realizar comunicaciones anónimas. También se podrán habilitar los canales internos para recibir información fuera del ámbito del artículo 2, aunque en estos casos no se aplicará la protección de la ley. El informante podrá indicar un medio seguro para recibir notificaciones.

4.3 Procedimiento del SII

El procedimiento del SII regula la gestión y tramitación de las comunicaciones recibidas a través del canal interno de información que se integra en el SII de Grupo Fedola. Se adjunta dicho procedimiento como Anexo I de esta política.

En el caso de comunicaciones relativas a hechos presumiblemente constitutivos de acoso moral, acoso sexual, acoso por razón de sexo, ciberacoso o al acoso por razón de orientación sexual, identidad de género y/o expresión de género, se plantearán y tramitarán conforme al protocolo aplicable en cada empresa.

En el caso de que los hechos objeto de la información pudieran ser indiciariamente constitutivos de delito deberá ponerse en conocimiento del Ministerio Fiscal o la Fiscalía Europea, según proceda.

4.4 Canales externos

Sin perjuicio del cauce preferente del mencionada canal interno para la comunicación de posibles incumplimientos recogidos en la ley de protección del informante, Grupo Fedola comunica que podrán informar ante la Autoridad Independiente de Protección del Informante, A.A.I., o ante las autoridades u órganos autonómicos correspondientes, de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación, ya sea directamente o previa comunicación a través del correspondiente canal interno de información

5.- RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN (RSII)

De conformidad con lo dispuesto en el artículo 5.1 de la Ley 2/2023, de 20 de febrero, el Consejo de Administración de Grupo Fedola es el responsable de la implantación del SII y del tratamiento de los datos personales. El RSII que ha sido designado por el Consejo de Administración es la persona titular de la dirección del departamento jurídico de Grupo Fedola, que desarrollará sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad. Además, tiene atribuida la gestión diligente del sistema interno de información y el tratamiento adecuado de las comunicaciones recibidas.

Tanto la designación como el cese del RSII se notificará a la Autoridad Independiente de Protección al Informante o, en su caso, a las autoridades u órganos competentes de las comunidades autónomas, en el ámbito de sus respectivas competencias.

El RSII asumirá diligentemente, y en ausencia de conflicto de interés, la resolución de los procedimientos iniciados a raíz de las informaciones recibidas a través del canal interno establecido, asegurando la adecuación del procedimiento. En caso de conflicto de interés, ausencia o enfermedad, las funciones serán desarrolladas por la persona que ostente el puesto de

Compliance penal, quien en el ejercicio de esa función estará sujeto a las mismas obligaciones y principios que el RSII.

6.- MEDIDAS DE PROTECCIÓN Y GARANTÍAS

6.1 Condiciones de protección
Se otorga protección a quienes comuniquen infracciones del artículo 2, siempre que:

- Tengan motivos razonables para creer que la información es veraz, aunque no aporten pruebas concluyentes.

- La comunicación cumpla con los requisitos legales.

6.2 Exclusiones de protección
No se protege a quienes comuniquen información:

- Rechazada por los canales internos o inadmisible.

- Relativa a conflictos personales entre individuos.

- Ya disponible públicamente o basada en rumores.

- Fuera del ámbito de aplicación de la ley.

6.3 Extensión de la protección
- A representantes legales de trabajadores en funciones de apoyo al informante.

- A personas físicas relacionadas con el informante (compañeros, familiares, etc.) que puedan sufrir represalias.

- A personas jurídicas relacionadas laboralmente con el informante.

- Casos de anonimato: Si un informante anónimo es identificado posteriormente y cumple con los requisitos legales, también será protegido.

- Informaciones a la UE: Las personas que informen sobre infracciones ante instituciones de la Unión Europea tienen los mismos derechos de protección que aquellas que usen canales externos.

6.4 Prohibición de represalias
Las represalias son actos u omisiones prohibidos por la ley que generan un trato desfavorable, colocando a la persona afectada en desventaja en el ámbito laboral o profesional por ser informante o haber hecho una revelación pública. Estas incluyen:

1. Medidas laborales, como despido, suspensión, no renovación o terminación anticipada de contratos, degradaciones, denegación de ascensos, cambios en condiciones laborales o no conversión de contratos temporales a indefinidos, salvo que sean justificadas por causas ajenas a la comunicación.

2. Daños personales, como perjuicios económicos, reputacionales, intimidación, acoso u ostracismo.

3. Evaluaciones o referencias negativas sobre el desempeño.

4. Difusión de información perjudicial, como inclusión en listas negras que limiten el acceso al empleo.

5. Negativa de derechos, como licencias, permisos o formación.

6. Discriminación o tratos injustos.

Las personas afectadas pueden solicitar protección dentro de los dos años posteriores al acto de represalia, con posibilidad de extender este plazo de forma excepcional, previa justificación.

6.5 Medidas de apoyo

Asesoramiento: Información gratuita e independiente sobre procedimientos, recursos, protección frente a represalias y derechos del informante.

a) Asistencia: Apoyo efectivo de las autoridades competentes y certificación de protección bajo la ley.
b) Asistencia jurídica: En procesos penales y civiles transfronterizos según normativa comunitaria.
c) Apoyo financiero y psicológico: En casos excepcionales, evaluados por la Autoridad Independiente de Protección del Informante.
d) Compatibles con la Ley de Asistencia Jurídica Gratuita para representación en procedimientos judiciales.

6.6 Medidas de protección

a) Exoneración de responsabilidad: No se considera que el informante infringe restricciones de revelación si actúa con motivos razonables, salvo en casos de responsabilidad penal. Se aplica también a representantes laborales sujetos a confidencialidad.
b) Acceso a información: No habrá responsabilidad por adquirir o acceder a información comunicada si no constituye un delito.
c) Presunción de represalia: En procedimientos judiciales, si el informante demuestra perjuicio tras comunicar, se presume como represalia, y la carga de prueba recae en quien adoptó la medida perjudicial.
d) Protección en procesos judiciales: Los informantes no serán responsables por comunicaciones protegidas, pudiendo justificar su acción como necesaria para revelar infracciones.
e) Derechos de las personas afectadas: Garantía de presunción de inocencia, defensa, acceso restringido al expediente, confidencialidad de identidad y datos del procedimiento.

Estas medidas buscan garantizar un entorno seguro y protegido para los informantes.

6.7 Medidas de protección de la persona afectada por una comunicación

Durante el expediente, las personas afectadas tienen derecho a la presunción de inocencia, defensa, acceso al expediente, confidencialidad de su identidad, y protección de los datos y hechos relacionados, al igual que los informantes.

7.- LIBRO-REGISTRO DE INFORMACIONES

El RSII dispondrá de un libro-registro de las comunicaciones recibidas y las investigaciones realizadas. Dicho registro se conservará preferentemente en soportes que garanticen su integridad, confidencialidad y no manipulación, y no es público, únicamente podrán acceder a él jueces y tribunales en el marco de un procedimiento judicial, por lo que el RSII asegurará la disponibilidad de la documentación, para atender los requerimientos de autoridades judiciales y organismos o entes públicos que vengan amparados por la normativa que resulte de aplicación. Los datos personales relacionados con las comunicaciones e investigaciones únicamente se conservarán durante el período que fuese necesario, que en ningún caso podrá superar los diez años.

Concluidas las actuaciones, el RSII, emitirá un informe que se reflejará en el libro registro y que contendrá al menos:

1. Una exposición de los hechos relatados junto con el código de identificación de la comunicación y fecha de registro
2. La clasificación de la comunicación a efectos de conocer su prioridad o no en su tramitación
3. Las actuaciones realizadas con el fin de comprobar la veracidad de los hechos
4. Las medidas adoptadas en su caso.
5. Las conclusiones alcanzadas y la valoración de los indicios que las sustentan.
6. Fecha de cierre

8.- PROTECCIÓN DE DATOS PERSONALES

8.1 Régimen jurídico del tratamiento de datos personales.

El tratamiento de datos personales en el marco de esta ley se rige por:

- 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
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

8.2 Límites del tratamiento

Solo se recopilarán datos necesarios; los irrelevantes o accidentales se eliminarán inmediatamente. Las categorías especiales de datos personales se suprimirán sin registro ni tratamiento.

8.3 Licitud del tratamiento
La licitud del tratamiento se basa en la existencia de un sistema interno de información (SII). Las revelaciones públicas también están protegidas si se cumplen condiciones específicas del GDPR.

8.4 Información a interesados
Los interesados deben ser informados sobre el tratamiento de sus datos y el derecho a mantener su identidad reservada. La persona mencionada en una denuncia no será informada de la identidad del informante.

8.5 Preservación de datos
Los datos solo se conservarán el tiempo necesario para decidir sobre una investigación. Si en 3 meses no se inicia una investigación, los datos serán eliminados o anonimizados.

8.6 Acceso a datos en el SII
Acceso limitado al RSII, recursos humanos, servicios jurídicos y delegados de protección de datos. Los datos podrán ser compartidos con terceros si es necesario para procedimientos sancionadores o penales.

8.7 Identidad del informante
Su identidad será confidencial y solo podrá revelarse a autoridades judiciales, fiscales o administrativas en investigaciones penales. Antes de cualquier revelación, se informará al afectado, salvo que perjudique la investigación.

ANEXO I.- PROCEDIMIENTO DE GESTIÓN DEL SII

1.- PROCEDIMIENTO DE COMUNICACIÓN DE ACTUACIONES IRREGULARES.

1.1 Identificación de una irregularidad.
El Sistema Interno de Información (SII) permite a cualquier persona vinculada a la empresa comunicar de forma anónima o identificada el conocimiento de ilícitos, irregularidades u omisiones. Estas denuncias serán gestionadas por el Responsable del SII (RSII), quien investigará y tomará medidas para prevenir futuras conductas similares.

Las comunicaciones pueden abarcar incumplimientos de obligaciones legales, protocolos internos, el Código de Conducta, o hechos con naturaleza antijurídica o delictiva.

Se incluyen en su alcance: las infracciones del Derecho de la Unión Europea, el Código Penal español o que afecten a intereses financieros de la UE; las infracciones penales o administrativas graves o muy graves, como las que causen perjuicio económico a la Hacienda Pública y Seguridad Social; y las infracciones del Derecho laboral en materia de seguridad y salud en el trabajo.

El SII no exige conocimiento técnico-jurídico de los hechos denunciados, ya que el RSII será responsable de determinar su naturaleza legal o administrativa.

1.2 Comunicación/Recepción de la comunicación.

Los canales internos de información estarán a disposición las 24 horas al día, 365 días al año, garantizando la máxima confidencialidad. Se exponen a continuación en orden de preferencia de uso, sin perjuicio de la voluntad de la persona informante:

a) App corporativa "Fedola Conecta" exclusiva para personas trabajadoras de todas las sociedades.
b) Herramienta informática disponible en el apartado "canal de denuncias" de la página web corporativa;
c) Correo electrónico canaldedenuncias@grupofedola.com.

Además de las vías informáticas anteriormente enumeradas, las denuncias podrán realizarse por los siguientes medios:

d) Por correo certificado con acuse de recibo, dirigido a Grupo Fedola, Calle Candelaria, Edificio Olympo, Nº 28, 1º piso, C.P. 38002, Santa Cruz de Tenerife, y dirigido a la atención del RSII.
e) Por vía telefónica, en el teléfono de las oficinas centrales de Grupo Fedola, número 922 151499, y marcando la extensión número 4 correspondiente al Departamento Jurídico, y a la figura del RSII.
f) Reunión presencial solicitada previamente a través de cualquiera de las vías anteriormente descritas.

Todos los canales internos garantizan la confidencialidad de las comunicaciones, pero el único canal que garantiza el anonimato entendido como la capacidad de informar sin ser identificado por ningún medio, es a través de la herramienta informática disponible en la web.

En el caso de comunicaciones relativas a hechos presumiblemente constitutivos de acoso moral, acoso sexual, acoso por razón de sexo, ciberacoso o al acoso por razón de orientación sexual, identidad de género y/o expresión de género, se plantearán y tramitarán conforme al protocolo aplicable en cada empresa. Sin perjuicio de lo anterior, los empleados también podrán presentar una comunicación de acoso directamente a través del canal interno de información, al igual que puede hacerlo cualquier otro informante de los previstos en el referido apartado 3 de la política del SII, en cuyo caso el RSII remitirá la comunicación al encargado de tramitar las denuncias por acoso según el protocolo de aplicación. El procedimiento de investigación y ulterior determinación de la existencia o no de una situación de acoso, se regirán por los procedimientos establecidos en cada protocolo de las sociedades del Grupo.

El canal interno de información se dará a conocer a través de la página web de Grupo Fedola y de la aplicación corporativa "Fedola Conecta".

Sin embargo, a solicitud del informante, también podrá presentarse mediante una reunión presencial dentro del plazo máximo de siete días desde la formulación de la comunicación.

El acceso y/o utilización del SII supone la aceptación íntegra y sin reservas de las normas de funcionamiento contenidas en la presente política, esto es, que el usuario/informante ha leído, comprendido y consiente.

Las comunicaciones verbales, incluidas las realizadas a través de reunión presencial o telefónicamente, se documentarán, previo consentimiento del informante, a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.

Sin perjuicio de los derechos que le corresponden de acuerdo a la normativa sobre protección de datos, se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

1.3 Requisitos mínimos de la comunicación.

En la medida de lo posible, la comunicación contendrá la siguiente información:

1. Datos identificativos de la persona informante, salvo que opte por formular la comunicación de manera anónima.

2. Datos de contacto del informante, con el fin de aclarar cualquier duda durante la instrucción y para mantener al informante informado.

3. Descripción del evento sospechoso lo más concreto posible detallando:

a. En qué consiste la conducta posiblemente irregular.

b. Personas presuntamente implicadas.

c. Fechas aproximadas de comisión de los hechos.

d. Medios por los que se ha realizado la posible conducta ilícita.

e. Área de la organización afectada.

f. ¿Alguien de la organización tiene conocimiento de los hechos?

g. ¿ha tratado de comunicar anteriormente los hechos?

El RSII podrá volver a contactar con el informante en caso necesario, para ampliar información o para que pueda aportar documentación. En el caso de que la comunicación esté fuera del ámbito objetivo del SII, el RSII archivará la comunicación, dando cuenta al informante del archivo de la misma. Para ello, es importante que el informante facilite algún método de comunicación a tal fin.

1.4 Anonimato

El SII de Grupo Fedola permite que las comunicaciones puedan llevarse a cabo de forma anónima.

No obstante, Grupo Fedola promueve que, al menos, que facilite un modo de comunicación para poder plantearle cuanta información se necesite para el esclarecimiento de los hechos y pueda establecerse un medio de comunicación entre el RSII y el informante.

A pesar de lo anterior, cuando se presenta una comunicación (anónima o no), Grupo Fedola asegura que el procedimiento de comunicación interna se llevará a cabo de una manera segura que garantice la confidencialidad de la identidad de la persona informante y otra información relacionada.

2.- PROCEDIMIENTO DE GESTIÓN COMUNICACIONES

2.1 Recepción de la información

Con el objetivo de obtener todos los datos necesarios para poder valorar la información y tomar las acciones oportunas, la comunicación deberá contar con los requisitos mínimos establecidos en la sección anterior. En este sentido, para asegurar la toma de datos adecuada, el RSII, deberá asegurarse de obtener todos los datos posibles de las comunicaciones y, en su caso, tratar de contactar con el informante para obtener todos los datos que se necesiten.

2.2 Registro y clasificación de la comunicación

Una vez recibida la comunicación, se le asignará un código de identificación único, y se clasificará al objeto de priorizar las comunicaciones recibidas atendiendo a los siguientes criterios de categorización: leve, grave, muy grave o improcedente.

Tanto la admisión a trámite de la comunicación, como la desestimación y su motivo, en su caso, serán comunicadas al informante, en un plazo máximo de 3 meses.

Los datos que se proporcionen a través del canal interno de información serán incluidos en un fichero de datos de carácter personal, que será tratado conforme a lo establecido en el Reglamento General de Protección de Datos y la normativa de aplicación.

En caso de recibirse diferentes comunicaciones de irregularidades sobre un mismo hecho o sobre hechos vinculados a una misma persona afectada por la comunicación, el RSII podrá acumular los distintos casos, asignando a la citada agrupación de expedientes la numeración del más antiguo.

En un análisis preliminar el RSII podrá proponer medidas relativas a comunicaciones urgentes, proponiendo en su caso medidas para mitigación del riesgo materializado o por materializar, y medidas de preservación de pruebas.

2.3 Trámite de admisión

Una vez registrada la información, el RSII, deberá comprobar si expone hechos o conductas que se encuentran dentro del ámbito material de aplicación.

Realizado este análisis preliminar, el RSII, decidirá admitir o inadmitir la comunicación, en un plazo no superior a diez días hábiles desde la fecha de

entrada en el registro de la información. También podrá remitir con carácter inmediato la información al Ministerio Fiscal.

a) Inadmitir la comunicación, en alguno de los siguientes casos:

1º Cuando los hechos relatados carezcan de toda verosimilitud

2º. Cuando los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico

3º. Cuando la comunicación carezca manifiestamente de fundamento o existan, indicios racionales de haberse obtenido mediante la comisión de un delito. En este último caso, además de la inadmisión, se remitirá al Ministerio Fiscal relación circunstanciada de los hechos que se estimen constitutivos de delito.

4º. Cuando la comunicación no contenga información nueva y significativa sobre infracciones en comparación con una comunicación anterior respecto de la cual han concluido los correspondientes procedimientos, a menos que se den nuevas circunstancias de hecho o de Derecho que justifiquen un seguimiento distinto.

5º. Cuando se trate de informaciones que afecten a la información clasificada o hayan sido declarados secreto o reservados.

La inadmisión se comunicará al informante dentro de los cinco días hábiles siguientes, salvo que la comunicación fuera anónima y el informante hubiera renunciado a recibir comunicaciones.

b) Admitir a trámite la comunicación

La admisión a trámite se comunicará al informante dentro de los cinco días hábiles siguientes, salvo que la comunicación fuera anónima y el informante hubiera renunciado a recibir comunicaciones.

c) Remitir con carácter inmediato la información al Ministerio Fiscal cuando los hechos pudieran ser indiciariamente constitutivos de delito o a la Fiscalía Europea en el caso de que los hechos afecten a los intereses financieros de la Unión Europea.

2.4 Desarrollo de la investigación

Una vez que se haya obtenido del informante toda la información relevante sobre los hechos comunicados, y admitida a trámite la comunicación, el RSII encomendará la investigación de la comunicación a la comisión de investigación, cuya composición variará en función de la estructura de la empresa de la que trate la comunicación al igual que los integrantes de la misma, que variarán en función de la unidad de negocio afectada.

El RSII en el momento de convocatoria de la comisión, deberá excluir a aquellos miembros que se encuentren en conflicto de intereses a tenor del contenido de la comunicación. En estos casos será sustituido por persona que ocupe cargo homólogo o su superior jerárquico directo.

Asimismo deberá valorar la posible externalización de la investigación cuando los hechos comunicados afecten a personas que ejerzan funciones

especialmente sensibles en la organización, como miembros de la Alta Dirección o del Órgano de Gobierno.

2.5 Procedimiento de instrucción

El expediente deberá incoarse en un plazo máximo de 5 días hábiles y acusar de recibo al informante en un plazo máximo de 7 días hábiles.

La apertura del expediente se realizará en una pieza individualizada, con la identificación del informante, en caso de haberse identificado, y de la persona afectada por la comunicación, la situación de riesgo comunicada y su tipificación de hecho contemplada en la legislación penal.

En todo momento la comisión intentará llevar a cabo la investigación con medios propios y, de no ser posible, recabará la ayuda de otros departamentos o áreas operativas. Si fuera necesaria la participación de otros departamentos, su ayuda será recabada y se les exigirá el cumplimiento con el deber de confidencialidad.

Asimismo, cuando lo considere necesario, la comisión de investigación se podrá apoyar para la tramitación e investigación de la comunicación recibida en asesores o expertos independientes externos a los que se exigirá también el deber de confidencialidad.

La comisión de investigación deberá emitir una propuesta de resolución preferiblemente en el plazo de 2 meses desde la apertura del expediente, autorizándose una prórroga de un mes adicional si fuera necesario, previa resolución motivada debidamente comunicada a la persona afectada por la comunicación, en el caso en que el expediente no se haya considerado secreto atendiendo a la gravedad de los hechos investigados.

La comisión de investigación deberá acordar la práctica de las diligencias necesarias para el esclarecimiento de los hechos, dejando constancia documentada de todas y cada una de las actuaciones realizadas.

El resultado de dicha investigación se plasmará en un informe de conclusiones.

Las actuaciones que siempre deben desarrollarse son:

1. Solicitar ratificación al informante, en caso que se pueda comunicar con el informante, y recabar información complementaria relevante, como documentos o testimonios.
2. Citar a personas internas o externas involucradas para informarles sobre la existencia de la comunicación, tomarles declaraciones por escrito y solicitarles información adicional útil, como documentos o testimonios.
3. Comunicar la apertura del expediente a las áreas o unidades de negocio afectadas, solicitándoles la información necesaria para esclarecer los hechos.
4. Realizar una entrevista con la persona o personas afectadas por la comunicación, permitiéndoles acudir acompañadas de una persona de confianza. La persona afectada por la comunicación será informada de las acciones u omisiones que se le atribuyen, y tendrá derecho a ser oída en cualquier momento.

5. La propuesta de resolución debe incluir un informe detallado sobre las diligencias llevadas a cabo, así como aquellas que no se hayan podido realizar. Además, se deben presentar conclusiones sobre si se ha cometido un delito penal o una conducta prohibida por la ley vigente, las políticas de cumplimiento normativo u otras políticas de la organización, así como las personas presuntamente responsables.
6. El informe de conclusiones se comunica a la persona afectada, quien tiene un plazo máximo de 10 días para presentar sus alegaciones. Una vez analizadas las alegaciones, el RSII emitirá su propuesta de resolución final al Consejo de Administración.

2.6 Resolución de la comunicación

Una vez elaborado el informe de conclusiones (en adelante, "informe"), la comisión de investigación podrá adoptar las siguientes decisiones:

a) Archivar la comunicación y cerrar la investigación, si se considera que no se han demostrado conductas irregulares o que la información, a pesar de haber sido requerido para su ampliación el informante, no cumple los requisitos de veracidad y claridad.
b) Remitir el informe a la dirección de la empresa que deberá decidir sobre la imposición de las sanciones disciplinarias correspondientes, en su caso, en base al informe redactado.
c) Remitir el informe al Consejo de Administración de Grupo Fedola que deberá decidir sobre la iniciación o no de las correspondientes acciones judiciales o administrativas, incluidas las acciones penales o de índole disciplinario/sancionador que, en su caso, procedan.

Si se tratara de la comisión de un delito, evaluar un posible fallo en los controles implantados en prevención de delitos penales, y proponer acciones de mejora.

El informe deberá contener las diligencias practicadas y aquellas que no se hayan podido practicar y las conclusiones sobre si se ha cometido un ilícito penal o conducta prohibida y sobre las personas presuntamente responsables.

El informante y la persona investigada recibirán una notificación con una breve explicación de los pasos dados y la conclusión del expediente. Se tendrá en cuenta en todo momento la naturaleza confidencial de la información y los derechos de las personas implicadas.

2.7 Terminación de las actuaciones

Una vez realizadas todas las actuaciones de investigación, la comisión instructora emitirá informe-propuesta con el siguiente contenido:

1. Una exposición de los hechos relatados junto con el código de identificación de la comunicación y la fecha de registro.
2. La clasificación de la comunicación a efectos de conocer su prioridad o no en su tramitación.
3. Las actuaciones realizadas con el fin de esclarecer los hechos.
4. Las conclusiones alcanzadas en la instrucción y la valoración de las diligencias y de los indicios que las sustentan, indicando la propuesta de actuaciones a llevar a cabo.

Tras dicho informe, el RSII adoptará alguna de las siguientes decisiones:

- Archivo del expediente, que será notificado al informante y a la persona afectada. En estos supuestos, el informante tendrá derecho a la protección prevista en la ley, salvo que, como consecuencia de las actuaciones llevadas a cabo en fase de instrucción, se concluyera que la información a la vista de la información recabada, debía haber sido inadmitida por concurrir alguna de las causas previstas en el presente procedimiento.
- Remisión al Ministerio Fiscal si, pese a no apreciar inicialmente indicios de que los hechos pudieran revestir el carácter de delito, así resultase del curso de la instrucción. Si el delito afectase a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.
- Traslado de todo lo actuado al Consejo de Administración del Grupo Fedola para la adopción de cuantas medidas crean que correspondan en su caso.

Este informe de conclusiones será archivado y custodiado por el RSII en el libro-registro.

3.- ELABORACIÓN DE INFORME ANUAL

El RSII elaborará un informe anual para evaluar el funcionamiento y la eficacia del Sistema Interno de Información (SII), incluyendo datos como:

- Número total de comunicaciones recibidas.
- Clasificación de las comunicaciones (leve, grave, muy grave, improcedente).
- Comunicaciones archivadas sin investigación por no cumplir requisitos mínimos.
- Comunicaciones archivadas tras investigación al no constituir conducta irregular.
- Comunicaciones investigadas que resultaron en acciones disciplinarias, distinguiendo si implicaron un procedimiento judicial.
- Tipología de las conductas irregulares detectadas.
- Áreas de negocio afectadas por las comunicaciones.

El RSII establecerá objetivos anuales de mejora para optimizar el SII y los procesos de investigación. El informe se utiliza para el seguimiento y mejora continua del sistema.

ANEXO II.- FORMULARIO DE COMUNICACIÓN DE INFORMACIONES RELATIVAS A 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.

Instrucciones para el envío:

- Asegúrese de completar toda la información relevante.
- Si se incluye documentación adicional, adjúntela junto con este formulario.
- Envíe el formulario al canal habilitado por la organización para recibir comunicaciones conforme a la Ley 2/2023 y a la política del sistema interno de información.
- El canal interno de información garantiza la confidencialidad de la información y del informante, en cumplimiento de la normativa vigente.

1. Datos del informante (si desea permanecer en el anonimato, deje esta sección en blanco)

Nombre y Apellidos: _____

DNI/NIE (si aplica): _____

Teléfono de contacto: _____

Correo electrónico: _____

2. Canal de comunicación elegido para el seguimiento del caso:

☐ Correo electrónico ☐ Teléfono

☐ Otro (especificar): _____

3. Relación del Informante con la organización o entidad afectada:

☐ Empleado/a

☐ Colaborador/a

☐ Proveedor/a

☐ Usuario/a

☐ Otro (especificar): _____

4. Datos de la entidad y/o persona afectada por la comunicación:

Nombre de la entidad/organización: _____

Nombre del área/departamento: _____

Persona/s implicada/s (si se conocen): _____

5. Descripción de la infracción normativa o acto de corrupción (Describa detalladamente los hechos que desea comunicar. Incluya fechas, lugares y cualquier información relevante.)

6. Pruebas o documentos adjuntos (si los hubiera):

☐ Adjunta documentación adicional.

☐ No dispongo de pruebas en este momento.

7. Declaración del Informante:

Declaro que la información proporcionada en este formulario es veraz y ha sido recopilada y comunicada de buena fe, en el marco de la Ley 2/2023, para informar sobre posibles infracciones normativas o actos de corrupción.

Firma del informante: _____

Fecha: _____

Aviso Legal

Este formulario se encuentra amparado por la Ley 2/2023 y su uso indebido puede dar lugar a responsabilidades legales. Las comunicaciones realizadas de mala fe o con intención difamatoria están sujetas a sanciones legales.

ANEXO III PROTOCOLO DE CONFIDENCIALIDAD

1. OBJETIVO

El objetivo de este protocolo es asegurar la confidencialidad y protección de los informantes cuando la comunicación se realice por canales que no estén integrados en el SII.

2. RESPONSABILIDAD DEL PERSONAL

Todo el personal de la organización tiene la responsabilidad de mantener la confidencialidad de las comunicaciones internas y proteger la identidad de los informantes. Esto incluye a los empleados, directivos y cualquier otra persona que pueda recibir o tener acceso a información relacionada con una comunicación.

3. PROCEDIMIENTO EN CASO DE RECEPCIÓN DE COMUNICACIONES POR CANALES NO OFICIALES

Si un miembro del personal recibe una comunicación por un canal no oficial, deberá:

a) No divulgar la identidad del informante. Es importante no revelar la identidad del informante a ninguna otra persona, incluyendo a otros miembros del personal.

b) Remitir la comunicación al responsable designado. El miembro del personal debe remitir inmediatamente la comunicación al RSII, proporcionando todos los detalles y la documentación recibida.

c) El RSII comunicará al informante acerca del procedimiento correcto, siempre que le sea posible. Asimismo informará que la comunicación ha sido recibida y que se está siguiendo el proceso adecuado para su gestión.

d) Seguimiento y monitoreo. El RSII llevará a cabo un seguimiento de la comunicación y tomará las medidas necesarias para garantizar que se siga el proceso adecuado de gestión de comunicaciones.

4. INFORMACIÓN Y SENSIBILIZACIÓN

Se informará a todas las personas trabajadoras sobre la importancia de la confidencialidad y el uso adecuado de los canales de información interna, para promover una cultura de confianza y respeto hacia los informantes.