

POLÍTICA DEL SISTEMA INTERNO DE INFORMACIÓN DEL GRUPO ZENNIO

AVISO LEGAL

La presente política aplica al Sistema Interno de Información (“**SII**”) de Zennio Avance y Tecnología, S.L., cuyo alcance incluye tanto a dicha compañía como a todas sus filiales con independencia del país en el que se encuentren domiciliadas, en adelante el “**Grupo Zennio**” o “**Zennio**”, de conformidad con el Art. 11 LPI, como se define más abajo.

La presente documentación es propiedad de Zennio Avance y Tecnología S.L. y no podrá ser objeto de reproducción parcial, tratamiento o uso distinto al de la gestión del SII del Grupo Zennio sin el permiso previo y por escrito de Zennio Avance y Tecnología S.L., titular de los derechos de propiedad intelectual.

Versión 2	Elaborada por:	Revisada por:	Aprobada por:
Área	Legal	Comité de Compliance	Administrador Único
Fecha	Octubre 2025	Octubre 2025	Octubre 2025

ÍNDICE DE CONTENIDOS

1. VERSIONES.....	3
2. MARCO NORMATIVO.....	3
3. ALCANCE Y OBJETIVOS.....	3
4. ROLES Y RESPONSABILIDADES.....	4
4.1 Empleados de Zennio y Terceros Relacionados.....	4
4.2 Órgano de Administración.....	4
4.3 Responsable del SII.....	4
4.4 Instructores Delegados.....	5
4.5 Comité de Compliance y Departamento Legal.....	5
4.6 Proveedor externo del Canal Ético.....	5
4.7 Conflictos de interés y suplencias.....	5
5. GESTIÓN DE COMUNICACIONES.....	6
5.1 Presentación de las Comunicaciones.....	6
5.2 Medidas de Protección.....	7
5.3 Gestión de Comunicaciones.....	9
5.4 Cierre de Comunicaciones.....	13
6. PROTECCIÓN DE DATOS PERSONALES.....	14

1. VERSIONES

Versión	Razón del Cambio	Página(s)	Fecha
1	Creación de la Política del Canal Ético.	Todas	01/03/2024
2	Actualización a la Política del Sistema Interno de Información, conforme 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.	Todas	01/10/2025

2. MARCO NORMATIVO

- Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (“**DPI**”).
- 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 (“**LPI**”).
- Real Decreto 1101/2024, de 29 de octubre, por el que se aprueba el Estatuto de la Autoridad Independiente de Protección del Informante, A.A.I.
- Cualquier otra normativa relacionada como, por ejemplo:
 - Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (“**CP**”).
 - Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de capitales y de la Financiación del Terrorismo (“**LPBCFT**”).
 - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (“**LOPDGDD**”).

3. ALCANCE Y OBJETIVOS

El Sistema Interno de Información (“**SII**”) es gestionado por Zennio Avance y Tecnología, S.L. para sí misma y sus filiales (“**Grupo Zennio**” o “**Zennio**”), garantizando que, en todas las comunicaciones recibidas, también las provenientes de fuera de la Unión Europea, se mantenga un nivel de protección a los informantes equivalente a la LPI, DPI y la normativa que las amplíe o sustituya.

El objetivo de la presente Política es regular el funcionamiento del Sistema Interno de Información del Grupo Zennio, permitiendo a empleados y terceros relacionados comunicar, de buena fe, aquellas infracciones del **(i)** Derecho de la Unión Europea; **(ii)** Legislaciones locales penales o administrativas; y **(iii)** Políticas y Procedimientos Internos de Zennio; que sean cometidas por empleados y/o colaboradores del Grupo Zennio. Todo ello con una doble finalidad:

- **Preventiva:** Desincentivar comportamientos irregulares al proporcionar un mecanismo para que cualquier miembro de la organización o tercero relacionado pueda comunicar posibles infracciones, fomentando así la conducta ética y el cumplimiento normativo.
- **Reactiva:** Facilitar la comunicación confidencial de posibles infracciones, permitiendo detectar y abordar a tiempo cualquier situación que pueda acarrear responsabilidad penal o administrativa para Zennio, así como asegurando que se adopten acciones correctivas.

Todas las comunicaciones deberán ser gestionadas bajo los principios de confidencialidad, independencia y ausencia de represalias.

4. ROLES Y RESPONSABILIDADES

4.1 Empleados de Zennio y Terceros Relacionados

- Comunicación de conductas irregulares: Todos los empleados de Zennio y terceros relacionados, es decir, colaboradores, proveedores, subcontratistas y clientes, tienen la obligación de reportar, de buena fe y lo más precisa posible, cualquier conducta irregular cometida por empleados o colaboradores de Zennio. Las comunicaciones falsas o malintencionadas podrán dar lugar a responsabilidades disciplinarias o legales.

4.2 Órgano de Administración

- Nombramiento y cese del Responsable del SII: El Órgano de Administración designará a una persona física que actuará como responsable del SII y, en concreto, se ocupará de la gestión del [Canal Ético](#) y de la investigación de cada comunicación recibida ("**Responsable del SII**").
- Marco normativo: El Órgano de Administración aprobará la presente Política del Sistema Interno de Información y sus normas relacionadas.
- Autonomía y medios: El órgano de administración garantizará que el Responsable del SII pueda ejercer sus funciones con autonomía, independencia y medios suficientes.
- Evaluación Anual: El Órgano de Administración evaluará anualmente la eficacia del SII, el cumplimiento de los plazos y las garantías de confidencialidad, mediante la revisión de los informes de las investigaciones, así como mediante cualquier otro medio de evaluación que considere pertinente, adoptando medidas de mejora en caso de detectar irregularidades.
- Responsable suplente: En caso de que el Responsable del SII sea objeto de la comunicación o deba abstenerse por conflicto de interés, actuará como responsable suplente en el orden indicado en el apartado 4.7.

4.3 Responsable del SII

- Gestión del SII: El Responsable del SII es la persona física que está a cargo de gestionar las comunicaciones recibidas por los Canales Internos de Información, y de garantizar la confidencialidad y la protección del informante.
- Instrucción y delegación: El Responsable del SII podrá instruir cada investigación él mismo o delegar en personas de otras áreas de más especializadas o, incluso, en proveedores externos de servicios bajo su supervisión y sujetos a una estricta confidencialidad.
- Informe y Notificación: El Responsable del SII debe elaborar un informe detallado sobre cada comunicación recibida y elevar sus conclusiones al Órgano de Administración para la toma de decisiones. También informará al Comité de Compliance, proporcionando los menores datos personales posibles, salvo que fuese estrictamente necesario, de cara a que dicha entidad ponga en marcha medidas de mejor dentro de la organización.
- Confidencialidad: El Responsable del SII tratará las comunicaciones y su instrucción bajo la más estricta confidencialidad, procurando que los terceros que participen en la investigación guarden un nivel equivalente de confidencialidad.
- Protección: El Responsable del SII no adoptará ninguna represalia contra los informantes, y promoverá las medidas necesarias para la protección de los informantes cuando sea necesario.
- Abstención: El Responsable del SII deberá abstenerse de intervenir en la instrucción de una investigación en caso de conflicto de interés con los hechos comunicados. En estos casos, los responsables suplentes intervendrán en el orden indicado en el apartado 4.7

4.4 Instructor delegado

- Instrucción delegada: El Instructor Delegado estará a cargo de la instrucción de aquellas comunicaciones que el Responsable del SII le delegue en cada momento, quedando sujeto a las mismas obligaciones que el Responsable del SII en cuanto a confidencialidad, no represalias y abstención en caso de conflicto de interés.

4.5 Comité de Compliance y Departamento Legal

- Soporte: El Comité de Compliance y el Departamento Legal podrán ser informados por el Responsable del SII sobre todas o algunas de las comunicaciones recibidas y deberán dar apoyo al Responsable del SII en la llevanza de las investigaciones, si este lo solicita. Asimismo, deben asumir la implementación de medidas correctivas dentro de la organización.
- Instructores Delegados: Asimismo, podrán asumir la instrucción de aquellas investigaciones en las que el Responsable del SII esté incurso en un conflicto de interés.
- Responsable del SII suplente: En caso de que el Responsable del SII sea objeto de la comunicación o deba abstenerse por conflicto de interés, actuarán como responsables suplentes en el orden indicado en el apartado 4.7.
- Confidencialidad, No represalias y Abstención: El Comité de Compliance y el Departamento Legal quedan sujetos a las mismas obligaciones que el Responsable del SII en cuanto a confidencialidad, no represalias y abstención en caso de conflicto de interés.

4.6 Proveedor externo del Canal Ético

- Recepción de comunicaciones: El proveedor externo será el responsable de la gestión técnica del [Canal Ético](#) por cuenta del Responsable del SII, siendo quien supervisará diariamente si han entrado comunicaciones en el [Canal Ético](#), si bien carecerá de poder de decisión sobre las investigaciones, pudiendo tan solo asesorar y, en el caso del art. 4.7, instruir la investigación.
- Remisión comunicaciones: El proveedor externo, tras revisar el contenido de la comunicación, remitirá su contenido íntegro al Responsable del SII. En caso de que el Responsable del SII sea objeto de la comunicación o deba abstenerse por conflicto de interés, remitirá la comunicación a los responsables suplentes en el orden indicado en el apartado 4.7.
- Soporte en la instrucción: El proveedor externo proporcionará al Responsable del SII apoyo para documentar adecuadamente las comunicaciones recibidas, hará seguimiento de plazos y dará apoyo al Responsable del SII en la llevanza de las investigaciones si este lo solicita.
- Confidencialidad, No represalias y Abstención: El Proveedor Externo queda sujeto a las mismas obligaciones que el Responsable del SII en cuanto a confidencialidad, no represalias y abstención en caso de conflicto de interés y, adicionalmente, suscribirá el correspondiente encargo de tratamiento de datos personales.

4.7 Conflictos de interés y suplencias

En caso de que el Responsable del SII sea objeto de la comunicación o deba abstenerse por conflicto de interés, el Comité de Compliance, el Departamento Legal e incluso el Órgano de Administración podrán actuar como responsables suplentes en el siguiente orden y siempre que no estén afectados por conflicto de interés alguno: **(1º) Comité de Compliance;** **(2º) Departamento Legal;** y **(3º) Órgano de Administración;** debiendo estos a su vez delegar la instrucción en uno de sus miembros.

En el caso excepcional de que todos los responsables suplentes sean objeto de la comunicación o tengan conflicto de interés, el proveedor externo se hará cargo de la instrucción de la investigación.

5. GESTIÓN DE COMUNICACIONES

5.1 Presentación de las Comunicaciones

5.1.1 Quién puede comunicar y qué tipo de conductas deben comunicarse.

- **Obligación de comunicar incumplimientos:** Cualquier empleado, colaborador o socio del Grupo Zennio, o aquellos terceros que mantengan relaciones comerciales con Zennio, que tenga conocimiento de un incumplimiento cometido por los empleados, colaboradores o socios de Zennio, en un contexto laboral o profesional, deberá comunicarlo inmediatamente a través del SII. Si el informante es el autor de la conducta infractora (autodenuncia), la comunicación podrá valorarse como atenuante interna, sin implicar exoneración automática de responsabilidad.
- **Comportamientos comunicables a través del SII:**
 - **Incumplimientos del Derecho de la UE:** *Conductas que vulneren la normativa europea en contratación pública, servicios y mercados financieros, blanqueo de capitales y FT, seguridad de productos y transporte, medio ambiente, salud pública, protección de consumidores, datos personales, intereses financieros de la UE o mercado interior (Art. 2 DPI).*
 - **Incumplimiento de las legislaciones locales:** *Conductas constitutivas de delitos o infracciones administrativas graves o muy graves (Art 2 LPI).*
 - **Incumplimiento de normativa interna de Zennio:** *Conductas que vulneren el Código Ético y/o las políticas internas y/o protocolos vigentes en cada momento.*
- **Comportamientos no comunicables a través del SII:** Los siguientes hechos no se consideran denunciabiles a través del SII:
 - **Conflictos interpersonales o de recursos humanos:** Los conflictos interpersonales menores (como roces, malentendidos o problemas de convivencia que puedan resolverse mediante organización interna), así como cuestiones administrativas ordinarias de la relación laboral (salario, turnos, condiciones, variables, etc.), que no presenten la gravedad suficiente como para constituir una infracción administrativa grave o muy grave, o un ilícito penal (acoso laboral, sexual, etc), deberán gestionarse directamente con el Depto. RRHH.
 - **Reclamaciones comerciales.**
 - **Informaciones públicas, que no contengan información nueva o sean reiterativas.**
 - **Informaciones falsas o no fundamentadas.**

5.1.2 Contenido de la comunicación

La comunicación debe incluir una descripción clara y detallada de los hechos, así como toda la documentación disponible para aclarar o respaldar la información proporcionada, en concreto:

- Datos del informante, salvo que haya optado por una comunicación anónima.
- Descripción de los hechos acontecidos.
- Fecha de los hechos.

- Nombre y apellidos de las personas citadas.
- Medios de prueba que tenga a su alcance y que puedan acreditar la realidad de los hechos y/o conductas objeto de comunicación.

5.1.3 Canales de comunicación disponibles

Canales Internos de Comunicación

- **Canal Ético (*vía preferente*):** Zennio pone a disposición de los informantes su “**Canal Ético**”, una web que permite realizar las comunicaciones por escrito a través de un sencillo formulario habilitado para realizar la comunicación de manera confidencial si el informante lo desea. Aunque la comunicación anónima puede dificultar la investigación si no se proporciona un medio de contacto seguro alternativo como, por ejemplo, un correo electrónico temporal. El Canal Ético es accesible a través de la página web de [Zennio](#) en el apartado “Canal Ético” del pie de la página, o bien directamente a través del siguiente enlace <https://centinela-canal.lefebvre.es/canal-denuncias/zennio>.
- **Verbalmente:** Las comunicaciones podrán realizarse también verbalmente, por vía telefónica o mediante una reunión presencial dentro del plazo máximo de siete días, a petición del informante. Las comunicaciones verbales, ya sean mediante reunión presencial o telefónicamente, serán documentadas de alguna de las maneras siguientes: **a)** mediante una grabación de la conversación, o **b)** a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla, se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación. El uso de esta vía de contacto está autorizado por la LPI, pero la naturaleza del canal verbal impide garantizar el anonimato. En caso de querer usar esta vía, la llamada o reunión deberá concertarse mediante el envío de un email a responsablesii@zennio.com.

Canales Externos de Comunicación

Además de los Canales Internos, también se podrán realizar las comunicaciones directamente a través de las siguientes vías, si bien se aconseja acudir a los Canales Internos en primer lugar:

- **Canal de la Autoridad Independiente de Protección al Informante (AINPI):** es posible dirigirse directamente a la AINPI a través de su canal oficial (https://whistleblowersoftware.com/secure/canal_externo_de_denuncias_AINPI). También será posible dirigirse a la autoridad regional, en el caso de que llegue a constituirse en el futuro, así como a los de las instituciones de la Unión Europea.
- **Otras autoridades:** Directamente a fuerzas de seguridad, ministerio fiscal, autoridades en materia laboral, seguridad social, medioambiental, etc.

5.2 Medidas de Protección

5.2.1 Protección de los Informantes

Toda persona que, de buena fe, realice una comunicación o informe sobre conductas potencialmente irregulares estará protegida contra medidas sancionadoras o represalias. Esta protección se extiende a las personas vinculadas al informante o quienes le asistan durante el proceso.

Si bien, para que la referida protección sea aplicable las informaciones aportadas deben basarse en la buena fe, ya que la ley no ampara a quien aporte informaciones falsas, tergiversadas, o que se han obtenido de manera ilícita.

A continuación, se resumen las **principales medidas de protección** reconocidas por la ley para las personas que informen de buena fe sobre irregularidades o incumplimientos:

- **No habrá sanciones por informar:** quien comunique o haga pública una infracción **no** podrá ser castigado ni responsabilizado por ello, siempre que haya actuado de buena fe y tuviera motivos razonables para pensar que era necesario hacerlo.
- **Acceso legítimo a la información:** las personas informantes no serán sancionadas por obtener o acceder a la información que comuniquen, siempre que no cometan un delito para conseguirla.
- **Límites de la protección:** la protección legal solo cubre los actos necesarios para comunicar o revelar la infracción. Si el informante realiza acciones que no guardan relación directa con esa comunicación o que exceden lo razonablemente necesario (como manipular pruebas, difundir información privada o cometer un delito), esas conductas no estarán protegidas y podrán generar responsabilidad.
- **Presunción de represalia:** si alguien sufre un perjuicio tras presentar una denuncia, la ley presume que ha sido una represalia, salvo que la empresa demuestre lo contrario.
- **Defensa ante los tribunales:** en caso de demandas (por ejemplo, por difamación, violación de secretos o conflictos laborales), los informantes podrán alegar su condición de denunciantes protegidos y no serán responsables si actuaron con buena fe y dentro del marco de esta política.

5.2.2 Protección de las personas objeto de la comunicación

Durante la tramitación del expediente las personas afectadas por la comunicación tendrán derecho a la presunción de inocencia, al derecho de defensa y al derecho de acceso al expediente en los términos regulados en esta ley, así como a la misma protección establecida para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

5.2.3 Confidencialidad

Zennio asume el compromiso de velar por que no se revele la identidad de la persona que realice la comunicación a través de los Canales Internos del SII, salvo que ésta preste su consentimiento de forma expresa o sea requerido por las autoridades competentes en el marco de una investigación externa. En este sentido, salvo las personas específicamente autorizadas para recibir, seguir o resolver las comunicaciones recibidas, nadie podrá conocer la identidad del comunicante ni cualquier otra información que se pueda deducir a cerca de su identidad.

En caso de que se vaya a proceder a la revelación de la identidad del informante, Zennio se lo notificará a este previamente, salvo que pudiera comprometer la investigación.

El Responsable del SII deberá informar al Órgano de Administración sobre sus conclusiones de cada investigación y también podrá informar al Comité de Compliance, Depto Legal y Depto. RRHH, proporcionando documentos pseudoanonimizados, salvo que sea imprescindible conocer la identidad de las personas citadas a los efectos de adoptar acciones disciplinarias, legales o medidas de mejora.

El personal del Proveedor Externo, el Responsable del SII y sus colaboradores (Comité de Compliance, Depto. Legal, etc) están sujetos a deber de confidencialidad, reflejado contractualmente, y adicionalmente se han implementado medidas técnicas y organizativas para fortalecer dicha confidencialidad.

Zennio no puede garantizar la confidencialidad de los datos y hechos comunicados a través de canales distintos a los establecidos, especialmente si es a través de miembros de la organización no responsables de esta materia. Si bien, Zennio se compromete a formar adecuadamente a su personal sobre esta materia para minimizar estas situaciones y promover el uso de cauces oficiales que mejor garanticen la confidencialidad y trazabilidad.

Por último, Zennio se compromete a perseguir cualquier vulneración del deber de confidencialidad mediante la adopción de sanciones disciplinarias y/o acciones legales.

5.2.4 Medidas técnicas

5.2.4.1 Plataforma del Canal Ético, recepción y custodia de las comunicaciones

El Canal Ético del Grupo Zennio es la herramienta informática cifrada (HTTPS), basada en GlobalSuite, en servidores ubicados dentro del Espacio Económico Europeo y gestionada por un proveedor externo, que almacena y registra las comunicaciones sin que Zennio acceda a la plataforma en ningún momento.

5.2.4.2 Verificación de conflictos de interés en comunicaciones del Canal Ético

Al recibir una comunicación a través del Canal Ético, el proveedor externo realiza una revisión inicial para comprobar que el Responsable del SII puede gestionar el caso al no ser objeto de la comunicación y no incurrir en conflicto de interés a priori.

- Si no detecta conflicto, remite el expediente al Responsable del SII.
- Si detecta conflicto, aplica el orden de suplencia previsto en el apartado 4.7 (**Comité de Compliance → Departamento Legal → Órgano de Administración**), verificando también que los suplentes no son objeto de la comunicación ni tienen conflicto de interés a priori.

Por este filtrado inicial de posibles conflictos de interés, el Canal Interno de uso preferente es el Canal Ético y no la comunicación verbal directa con personal de la organización.

5.2.4.3 Conservación y eliminación segura de datos

Los expedientes generados en las investigaciones de las comunicaciones recibidas por cualquiera de los canales internos serán conservados bloqueados durante un plazo máximo diez años, salvo procedimientos judiciales o administrativos abiertos. Una vez finalizado el plazo, se realizará el borrado de los datos tanto del Canal como de los sistemas de Zennio.

5.2.4.4 Formación y controles internos del proveedor

El proveedor externo garantiza que todo su personal con acceso a la plataforma está formado en seguridad de la información, protección de datos y confidencialidad, y que solo el personal estrictamente necesario puede intervenir en la gestión de las comunicaciones recibidas.

5.3 Gestión Comunicaciones

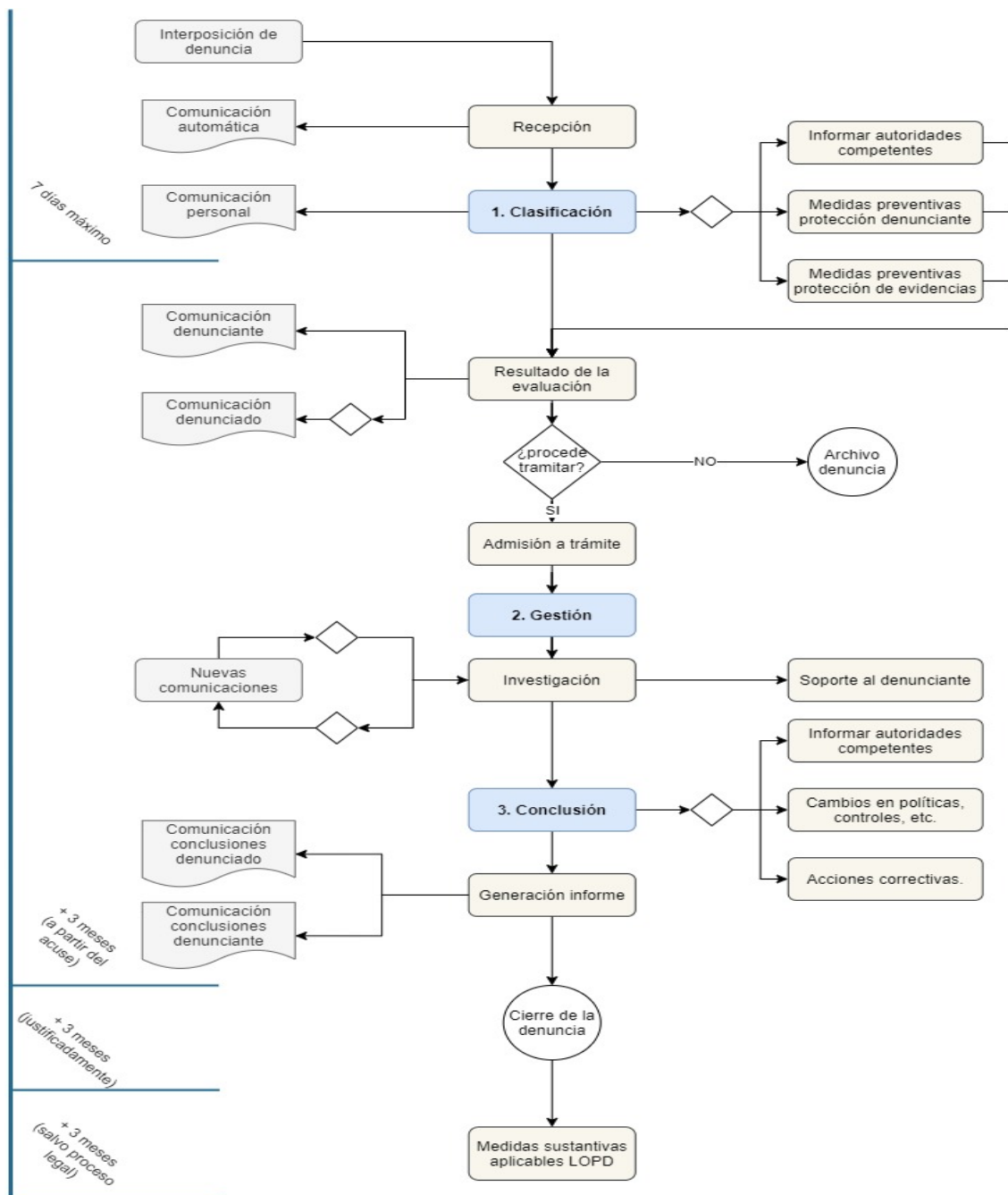
ACTIVIDADES			
FASE	ACCIÓN	DESCRIPCIÓN	RESPONSABLE
1	Recepción de comunicación	- La información/comunicación se podrá recibir por escrito a través del Canal Ético. - Se proporcionará al informante una copia de la presente Política mediante su inclusión en la plataforma informática del Canal Ético. - Si la comunicación se remite por canales distintos al oficial o a través de miembros del personal no responsable de su gestión, se informará al personal no responsable que haya intervenido sobre su obligación de guardar la debida confidencialidad, advirtiéndole de la obligación del receptor/a de remitir inmediatamente cualquier información adicional sobre la comunicación al Responsable del SII bajo pena de una infracción muy grave. - Recibida la comunicación a través del SII se verificará si es anónima o identificada y si indica un domicilio, teléfono o email para recibir las notificaciones. - Si el informante se identifica, se reservará su identidad en los términos del artículo 33 Ley protección informante, sin revelarla a terceras personas.	Responsable del SII

		6. La comunicación que se reciba en la plataforma informática será remitida por el Proveedor Externo al Responsable del SII o, en su defecto o por imposibilidad de este, al responsable suplente que le sustituya conforme al apartado 4.7, es decir, (1º) el Comité de Compliance, (2º) el Departamento Legal o (3º) el Órgano de Administración. Solo en caso de imposibilidad de contactar con ninguno de los tres anteriores será el Proveedor Externo quien gestione dicha comunicación. 7. En caso de que se habilite la opción de comunicación verbal (presencial, telefónica o por mensaje de voz): • Se advertirá que la comunicación será grabada e informará sumariamente del contenido de la presente Política, indicándole donde puede encontrar una copia. • Se documentará la conversación mediante grabación en formato seguro, duradero y accesible, o mediante transcripción completa y exacta. • Sin perjuicio de sus derechos en materia de protección de datos, se ofrecerá al informante oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción del mensaje. 8. Se identifique o no el informante, se le recomendará que facilite un modo de mantener la comunicación o de pedirle información adicional para la investigación. 9. Se registrará en el SII, asignándole un código. 10. El acceso al SII se limita a: • Responsable interno del sistema y, en su caso, a quien lo gestione directamente y a los proveedores externos que eventualmente se designen. • Instructor/a designado/a • Responsable de RRHH en el ámbito de medidas disciplinarias • Responsable servicios jurídicos, si se deben adoptar medidas legales • Delegado de Protección de datos.	
2	Acuse de recibo	1. En un máximo de 7 días hábiles desde recepción, la propia herramienta acusa recibo de la comunicación, si el informante se identifica. Si es anónima y/o ha renunciado a recibir comunicaciones no.	Proveedor Externo
3	Admisión o no a trámite	1. En todo caso se respetará presunción de inocencia, derecho a ser oído y honor de personas investigadas 2. Registrada la información se comprobará si expone hechos o conductas dentro del ámbito de aplicación recogido en la presente Política del SII. 3. En un máximo de 10 días hábiles desde fecha registro se decidirá: • Si se inadmite por: • Falta de verosimilitud • Hechos no constitutivos de infracción. • Carencia manifiesta de fundamento o indicios racionales de haberse obtenido mediante la comisión de un delito. • Si no contiene información nueva y significativa sobre infracciones comunicadas anteriormente sobre las que se haya concluido el correspondiente procedimiento, salvo que se den	Responsable interno del SII.

		nuevas circunstancias de hecho o de Derecho que justifiquen un seguimiento distinto. La inadmisión se notificará de forma motivada, salvo si es una comunicación anónima y/o el informante ha renunciado a recibir comunicaciones. • Si se admite. La admisión se notificará, salvo si la comunicación es anónima y/o el informante ha renunciado a recibir comunicaciones, de manera fundamentada. Asimismo, la comunicación se remitirá de inmediato al Ministerio Fiscal si los hechos contienen indicios claros de delito. 4. Durante todo el proceso de admisión o inadmisión de la comunicación se excluirán aquellas personas que puedan tener conflicto de interés con el contenido de la comunicación.	
4	Instrucción	1. El instructor/a, una vez admitida a trámite la denuncia, enviará el acta de admisión al Proveedor Externo que modificará la comunicación a estado "Investigando". 2. El Instructor/a categorizará la denuncia en coordinación con la categorización que haya realizado el informante. 3. El instructor/a podrá apoyarse en el Comité de Compliance, el Departamento Legal y el Director de RRHH, así como en personal especialista con carácter excepcional, durante la investigación. 4. Comprenderá las actuaciones necesarias para comprobar la verosimilitud de los hechos 5. Garantizará que la persona afectada por la información: • tenga noticia de esta y de los hechos relatados de manera sucinta; que se le informe de las acciones u omisiones que se le atribuyen, y a ser oída en cualquier momento. Dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación, si su aportación al inicio puede facilitar ocultación, destrucción o alteración de las pruebas. • se le informe del tratamiento de sus datos personales. • pueda presentar alegaciones por escrito. Esta información podrá darse en el trámite de audiencia • una entrevista, con respeto a la presunción de inocencia, invitando a exponer su versión de los hechos y a aportar las pruebas que considere adecuadas. • acceso al expediente sin revelar la identidad del informante, pudiendo ser oída en cualquier momento, y comparecer asistida de abogado/a. • En ningún caso se comunicará a los afectados la identidad del informante ni se dará acceso a la comunicación.	Responsable del SII o Instructor/a designado/a
5	Terminación de las actuaciones y respuesta al informante	1. Plazo máximo para finalizar actuaciones y responder al informante: 3 meses desde el registro de la información. Salvo casos de especial complejidad que requieran ampliación de plazo, (hasta un máximo de otros 3 meses más). 2. Lo expuesto con la salvedad de aquellos supuestos específicos que legalmente tengan establecidos otros plazos (como por ejemplo, en materia de acoso sexual y acoso por razón del sexo en el trabajo).	Responsable del SII/Instructor/a designado/a

		3. Cualquiera que sea la decisión, se comunicará al informante, salvo que haya renunciado a ello o que la comunicación sea anónima 4. Terminada la instrucción se emitirá un informe con: • Los hechos relatados, el código de identificación de la comunicación y la fecha de registro • La clasificación de la comunicación a efectos de conocer su prioridad o no en su tramitación • Las actuaciones realizadas para comprobar la verosimilitud de los hechos y las conclusiones, la valoración de las diligencias y los indicios que las sustentan 5. La decisión comprenderá una de estas opciones: • Archivo del expediente, notificándolo al informante y a la persona afectada. Dicho archivo podrá decretar la ausencia de verosimilitud o de ausencia probatoria o de incumplimiento de la comunicación recibida. • O en el supuesto de probarse que los hechos de la comunicación resultaren ser ciertos, evidenciándose con ello un incumplimiento o infracción normativa, proponerse la adopción de las medidas pertinentes conforme a la legislación laboral y resto de obligaciones civiles y mercantiles de aplicación 6. El informante tendrá derecho a la protección de la ley salvo que, de la instrucción, se concluya que la información debía haber sido inadmitida por los motivos del apartado 3.3 anterior. 7. Remisión al Ministerio Fiscal si, pese a no apreciar inicialmente indicios de delito, sí se aprecian en la instrucción. 8. Una vez dispuesta la terminación de la instrucción y adoptada la decisión pertinente acerca de la comunicación recibida, el Responsable del Sistema será el encargado de enviar el informe de cierre al Proveedor Externo que modificará el estado a "finalizado".	
6	Conservación y destrucción de datos personales	1. No se tratarán datos personales no necesarios para el conocimiento e investigación de los hechos comunicados, procediéndose, en su caso, a su inmediata supresión, al igual que los datos personales referidos a conductas no incluidas en el ámbito de aplicación de la ley. Si la comunicación incluye categorías especiales de datos personales, solo se tratarán cuando resulte estrictamente necesario para investigar los hechos; en caso contrario, se suprimirán inmediatamente. 2. Si se acreditara que la información facilitada o parte de ella no es veraz, se suprimirán desde el momento en que se tenga constancia de dicha circunstancia, salvo que la falta de veracidad pueda constituir un ilícito penal, en ese caso se guardará la información el tiempo necesario durante el que se tramite el procedimiento judicial. 3. Los datos personales del denunciante, así como de los empleados/as y terceros solo se conservarán en el SII durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados. 4. Pasados 3 meses desde la introducción de los datos, se suprimirán del sistema de denuncias, salvo que la finalidad de conservarlos sea dejar evidencia del funcionamiento del SII en cuyo caso deberán ser bloqueados.	Responsable del SII y Proveedor Externo

Flujograma



5.4 Cierre de la Comunicación

El Responsable del SII deberá completar la investigación de la comunicación en el plazo de tres meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante, a tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación, salvo casos que requieran una ampliación del plazo en otros tres meses adicionales.

Una vez completada la investigación, el Responsable del SII emitirá el correspondiente informe de cierre indicando sus conclusiones las medidas acordadas (informar a las autoridades, adoptar medidas disciplinarias o judiciales y/o acciones de mejora) y lo comunicará al informante y a las personas investigadas, procediendo al cierre y archivo de la comunicación.

6. PROTECCIÓN DE DATOS PERSONALES

Responsable del tratamiento	Zennio Avance y Tecnología, S.L., con domicilio en Toledo (España), actuando como responsable del Sistema Interno de Información (SII) propio y de las filiales del Grupo Zennio.
Encargado del tratamiento	Proveedor externo independiente que gestiona la plataforma del Canal Ético, conforme a contrato de encargo de tratamiento (art. 28 RGPD).
Datos	Datos identificativos y de contacto del informante, si no es anónimo; datos de personas implicadas o mencionadas en la denuncia; y datos adicionales aportados en la investigación (documentos, correos, etc.).
Finalidad	Gestionar las comunicaciones recibidas a través del SII: recepción, verificación de conflictos de interés, análisis, investigación, resolución y archivo.
Base de legitimación	Cumplimiento de una obligación legal (art. 6.1 c RGPD) y misión de interés público (art. 6.1 e RGPD), conforme a la LPI.
Destinatarios	Autoridades judiciales o administrativas competentes; responsables internos designados por Zennio (SII, Comité de Compliance, Departamento Legal u Órgano de Administración); proveedor externo del Canal Ético.
Transferencias internacionales	No previstas. En caso necesario, se aplicarán cláusulas contractuales tipo u otros mecanismos del art. 44-49 RGPD.
Plazo de conservación	3 meses si no se inicia la investigación. Durante el tiempo necesario para la investigación en curso y, posteriormente, bloqueados durante el tiempo en que puedan exigirse responsabilidades con un máximo de diez años (art. 26 Ley 2/2023).
Medidas de seguridad	Plataforma web segura (HTTPS), accesos restringidos, medidas contractuales de confidencialidad reforzada, bloqueo de datos, accesos con contraseña, omisión de nombres de personas en informes, etc.
Derechos	Acceso, rectificación, supresión, limitación, oposición y portabilidad, mediante solicitud a dpo@zennio.com . Asimismo, podrá presentar reclamación ante la Agencia Española de Protección de Datos (www.aepd.es).