PROCEDIMIENTO DE GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN

grupo solutia

ÍNDICE

1. OBJETO

El presente procedimiento tiene por finalidad el desarrollo e implementación del Sistema de Información de Grupo Solutia Tecnología S.L. (en adelante **Grupo Solutia**), Solutia Innovaworld Technologies S.L., Solutia Digital Health S.L., Solutia Solutions Services S.L., y Solutia Cybersecurity S.L. con el con el fin de ofrecer un cauce seguro para empleados, proveedores y clientes de **Grupo Solutia,** para poder denunciar aquellos hechos y conductas relacionadas con su actividad que puedan ser constitutivas de infracciones del Derecho de la Unión Europea, de delito o infracción administrativa, o supongan el quebrantamiento de la normativa interna de la compañía dictada en desarrollo del Sistema de Compliance Penal, en especial, del Catálogo de Conductas Prohibidas.

Este procedimiento, ha sido aprobado por el Órgano de Administración, y con él se garantiza el respeto a la normativa de protección de datos y se desarrollan e implementan los principios dispuestos en 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.

2. ÁMBITO DE APLICACIÓN

Grupo Solutia pone a disposición de sus empleados, proveedores, clientes, así como cualquier tercero con relación directa e interés comercial o profesional (en adelante, “interesados”), con independencia de su nivel jerárquico y de su ubicación geográfica o funcional, el Sistema de Información Interna, como cauce confidencial para la comunicación de incumplimientos en las siguientes materias:

- Hechos que puedan ser constitutivos de delito.
- Hechos que pueden ser constitutivos de soborno.
- Hechos que puedan ser constitutivos de infracción administrativa
- Conductas que supongan la infracción de la normativa interna en materia de prevención de riesgos penales, o antisoborno, en especial, del Catálogo de Conductas Prohibidas, del Código de Conducta Interno, y del Código Ético de Proveedores.
- Hechos que puedan suponer la infracción del Derecho de la Unión Europea.

Las comunicaciones realizadas a través del Sistema de Información Interna se referirán exclusivamente a conductas que pudieran efectivamente afectar de forma razonable al mantenimiento o desarrollo de la relación laboral, comercial o profesional entre **Grupo Solutia** y sus empleados, proveedores o terceros con los que mantiene una relación directa, así como a la reputación de **Grupo Solutia**, o que pudieran tener consecuencias legales para ésta.

No son objeto de este Canal:

1. Las denuncias que puedan venir referidas al ámbito de la vida privada de las personas anteriormente citadas.
2. Las reclamaciones de clientes referidas a aspectos concretos de la prestación de servicios de **Grupo Solutia** ajenos a las materias anteriormente dispuestas.
3. Los conflictos y las cuestiones laborales y de gestión de recursos humanos de la Compañía, que deberán ser canalizados a través de los cauces ordinarios y del departamento de Recursos Humanos.

Queda excluido del ámbito de aplicación del Sistema de Información Interna, de conformidad a lo dispuesto en el artículo 2 de la Ley 2/2023, aquellos hechos que puedan entrar dentro del ámbito de las materias objeto del canal que se conozcan por razón de una profesión en la que opere el deber legal de secreto profesional. A estos efectos, se aclara que dentro de la entidad solo se encuentran comprendidos en este ámbito el personal que desarrolla actividades de abogacía y sólo en el desempeño de dicha actividad.

El Sistema de Información Interna es un canal independiente de los canales de comunicación habituales de **Grupo Solutia** con sus empleados, proveedores y terceros con los que mantiene una relación laboral, comercial o profesional directa, y no los sustituye.

3. COMPETENCIA DE LA GESTIÓN DEL SISTEMA DE INFORMACIÓN INTERNA

El Sistema Interno de Información será gestionado por el Compliance Officer de **Grupo Solutia**, que será el responsable del sistema a los efectos de lo previsto en el artículo 8 de la Ley 2/2023. Éste es el encargado de impulsar las investigaciones que serán necesarias y de proponer, en su caso, las medidas de reparación, prevención y concienciación oportunas.

El Compliance Officer actuará en todo momento de forma independiente y autónoma, con el máximo respeto al principio de confidencialidad de las comunicaciones recibidas, de las personas afectadas y de la documentación que, en su caso, se genere.

4. MEDIOS PARA REALIZAR LA COMUNICACIÓN

Se podrá hacer uso del Sistema de Información Interna a través del canal Ético, publicado en la propia página web de **Grupo Solutia**: https://gruposolutia.com/canaletico.

El cauce de comunicación aquí dispuesto permite la realización de denuncias por escrito y con carácter confidencial a lo largo de toda la tramitación del procedimiento, tanto para el denunciante como para el denunciado, permitiendo una comunicación bidireccional entre el Compliance Officer y el denunciante, aunque éste haya planteado la denuncia de forma

anónima, y el Compliance Officer y el denunciado, caso de que se tengan sus datos para notificaciones.

5. CONTENIDO DE LAS COMUNICACIONES

A fin de garantizar el rigor de la investigación y confidencialidad en el tratamiento de las comunicaciones, estas deberán contener como mínimo, y según los casos, las siguientes menciones:

- Identificación de la persona que realiza la comunicación; dicha identificación será voluntaria.
- Vinculación del interesado con **Grupo Solutia**.
- Hechos que se desea poner en conocimiento del Compliance Officer, concretando en la medida de lo posible la vulneración de la normativa que se aprecie.
- Identificación de la persona o personas a las que se imputa el incumplimiento y datos para contactar con ellas, si se conocen.
- Pruebas sobre los hechos relatados, siempre que sea posible.

Los interesados deberán proporcionar la información específica y objetiva que sea necesaria para determinar si el objeto de su comunicación se encuentra dentro del alcance del Sistema Interno de Información, evitando facilitar datos personales que puedan revelar origen étnico o racial, opiniones políticas, convicciones religiosas, filosóficas, afiliación sindical, o datos biométricos o relativos a la salud, o a la orientación sexual del interesado o de cualquier otra persona física, salvo que se traten de datos indispensables para entender el alcance de la comunicación.

El Compliance Officer gestionará igualmente aquellas comunicaciones que omitan la identificación del interesado por haberse efectuado de manera anónima.

6. TRAMITACIÓN E INVESTIGACIÓN DE LAS COMUNICACIONES

6.1 Recepción y admisión de las comunicaciones.

Las comunicaciones realizadas a través del Sistema Interno de Información serán recibidas por el Compliance Officer a través de la plataforma del Sistema Interno de Información, accesible a través del sistema de información habilitado al efecto.

Una vez generada la denuncia, el denunciante recibirá los datos necesarios para hacer el seguimiento del estado de tramitación de la misma, que podrá consultar:

- Si la denuncia fue anónima: a través de la misma plataforma mediante la que denunció, introduciendo el código de denuncia que se generó.

- Si se facilitaron datos: llegará un correo electrónico indicando el cambio del estado de tramitación y en cualquier caso, también se tendrá acceso a la plataforma del Sistema Interno de Información para acceder a todas las comunicaciones.

El Compliance Officer recibirá y gestionará las denuncias a través de la plataforma de gestión del Sistema Interno de Información. Recibida la denuncia, generará el acuse de recibo en un plazo no superior a 7 días hábiles, que será accesible para el denunciante a través del propio Sistema Interno de Información. Para ello, el denunciante deberá introducir el código de denuncia en el canal y obtendrá el acceso a su expediente. Caso de que el denunciante facilitara su correo electrónico, llegará una alerta al mismo que le avisará de los cambios en el estado de tramitación del expediente.

A continuación, el Compliance Officer comprobará, en primer lugar, si la comunicación recae dentro del ámbito de aplicación del canal, y si ésta es fundada, en cuyo caso abrirá el correspondiente expediente.

En otro caso, si la comunicación no entra dentro del ámbito de aplicación del Sistema Interno de Información, o no se encuentra debidamente fundada, se ordenará su archivo inmediato, cuestión que se comunicará al denunciante a través del Sistema Interno de Información.

Se considerarán infundadas todas aquellas denuncias que no vengan acompañadas de un mínimo probatorio exigible o indicios razonables de la comisión de los hechos y sobre las que no sea posible la obtención de prueba alguna, así como aquellas que sean manifiestamente falsas.

El plazo para comunicar el archivo de la denuncia no podrá exceder de 3 meses desde la producción del acuse de recibo al denunciante.

Se ruega a todas las personas incluidas en el ámbito de aplicación de este procedimiento que realicen un **uso responsable** del Sistema Interno de Información, omitiendo emplear dicho cauce en materias que no son su objeto.

6.2 Apertura del expediente.

Si tras el análisis de los hechos contenidos en la comunicación, el Compliance Officer considera que concurren indicios razonables de la existencia de incumplimientos, se acordará la apertura del expediente y el inicio de la correspondiente investigación interna.

Paralelamente a la apertura del expediente y a la incoación de la investigación por el Compliance Officer, éste podrá adoptar medidas adicionales urgentes, a fin de evitar el riesgo en el desarrollo de la investigación, o que sea precisa para proteger al interesado.

6.3 Investigación interna.

En el desarrollo de la investigación, el Compliance Officer podrá recabar la información y documentación que consideren oportuna de cualquier departamento, atendiendo en cada caso a la relevancia y naturaleza de los hechos comunicados.

El Compliance Officer podrá practicar cuantas investigaciones se estimen necesarias a la luz de cada caso concreto, con el fin de determinar la verosimilitud de los hechos comunicados.

En estas actuaciones, el Compliance Officer podrá dirigirse al denunciante para solicitar más pruebas y datos sobre los hechos denunciados, o aclaraciones a los mismos de ser estrictamente necesario para proseguir las actuaciones.

La petición de colaboración del denunciante deberá efectuarse sólo en casos en que sea estrictamente necesario a fin de proseguir la investigación.

Caso de que las actuaciones no puedan proseguir sin la colaboración del denunciante, se procederá al archivo de éstas siempre y cuando transcurra un periodo de 3 meses desde que se solicitó información a éste. En ese caso, se remitirá la correspondiente comunicación de archivo de la actuación al denunciante.

Cuando la comunicación ponga en conocimiento incumplimientos especialmente graves o cuando las circunstancias del caso así lo requieran, el Compliance Officer adoptará las medidas oportunas para garantizar en todo momento la objetividad de la investigación. Si la comunicación implica directa o indirectamente a alguno de los miembros del Compliance Officer, éste deberá abstenerse de participar en la investigación y resolución de la misma. Si tras la investigación resulta implicado directa o indirectamente alguno de los miembros del Compliance Officer, éstos deberán abstenerse de participar en la resolución de la comunicación, poniéndolo en conocimiento del Órgano de Compliance.

Sin perjuicio de lo anterior, el Compliance Officer podrá externalizar la instrucción de la investigación en aquellos casos en que resulte adecuado dada la naturaleza, gravedad y complejidad de la comunicación.

6.4 Información y trámite de audiencia.

Las personas cuyas conductas hubieran sido identificadas como presuntamente irregulares en la comunicación, serán informadas por el Compliance Officer de dicha circunstancia y del tratamiento de sus datos, **en el tiempo y forma que se consideren adecuados para garantizar el buen fin de la investigación.**

A partir de dicho momento, estas personas adquirirán la condición de interesado, y podrán plantear los argumentos, alegaciones y pruebas que a su derecho convengan, en cualquier momento antes de la adopción de la resolución que ponga fin al procedimiento.

En caso de no poder contactar con el denunciado, resultará imposible la realización del trámite de audiencia.

6.5 Finalización extraordinaria del procedimiento por comisión del delito.

En caso de que los hechos denunciados puedan ser constitutivos de delito, se comunicará al Órgano de Gobierno para que éste lo ponga en conocimiento del Órgano de Gobierno de la entidad y proceda a la denuncia de los hechos ante el Ministerio Fiscal o la Fiscalía Europea (según proceda), dando por cerrada la investigación interna desde ese momento.

En estos casos, debido al potencial riesgo de destrucción de pruebas, **se omitirá la realización del trámite de audiencia al denunciado en protección de un interés jurídico mayor, pudiendo realizar éste las alegaciones que estime oportunas ante las autoridades.**

7. FINALIZACIÓN ORDINARIA DE LA INVESTIGACIÓN: CONCLUSIONES Y RESOLUCIÓN DE LA INVESTIGACIÓN

Tras la investigación y una vez concluido el trámite de audiencia caso de que este haya podido producirse, el Compliance Officer elaborará la correspondiente resolución, que deberá contener:

- Descripción de la investigación realizada
- Hechos probados en la investigación
- Conclusiones, en las que se podrá declarar:
  - La existencia del incumplimiento, en cuyo caso se podrá adoptar las siguientes medidas:
    - Propuesta de medidas de reparación del daño y corrección de la situación, así como de prevención para el futuro.
    - Propuesta, en su caso, de medidas disciplinarias, que podrán ir desde el apercibimiento hasta el despido dependiendo de si el incumplimiento ha sido leve, grave o muy grave de conformidad con el procedimiento disciplinario del sistema de prevención de riesgos penales.

En este caso, las conclusiones alcanzadas por el Compliance Officer se elevarán al Órgano de Gobierno de la entidad, que adoptarán la decisión final.
Una vez efectuado la anterior, en caso de que proceda, se notificará al denunciante a través de la plataforma del Sistema Interno de Información. El denunciado también será notificado de la decisión final que se adopte, pudiéndose usar la propia plataforma del Sistema Interno de Información, así como cualquier otro medio de comunicación (correo electrónico o postal), que garantice la recepción de dicha resolución.

La resolución definitiva deberá ser trasladada, en el caso que proceda, al departamento correspondiente para que éste adopte y aplique las medidas de remediación que sean pertinentes, de las que se dará cuenta al Compliance Officer.

Toda medida disciplinaria que se adopte deberá ser autorizada por el Órgano de Gobierno.

- El archivo del caso, en el supuesto de que se verifique que no ha existido incumplimiento. En este último caso, la propuesta de resolución del Compliance Officer necesitará ser confirmada por el órgano de administración.

Como garantía de la confidencialidad del procedimiento, el Compliance Officer únicamente comunicará el contenido de la resolución y el tipo de medidas que, en su caso se establezcan, a los interesados del mismo, y cuando sea procedente, al departamento o área correspondiente. Cuando proceda la adopción de medidas disciplinarias, se pondrá en conocimiento a la alta dirección para la imposición de las mismas.

8. CONSERVACIÓN, CUSTODIA Y ARCHIVO DE LA INFORMACIÓN

De conformidad al artículo 26 de la Ley 2/2023, se debe disponer de un libro-registro de las informaciones recibidas y de las investigaciones internas a que haya dado lugar, garantizando los requisitos de confidencialidad de dicha ley.

Este registro no será público y únicamente a petición razonada de la autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquella, podrá accederse total o parcialmente a su contenido.

El Compliance Officer mantendrá un registro actualizado de todas las comunicaciones recibidas, así como, en su caso, de las investigaciones internas llevadas a cabo y de las medidas adoptadas durante un plazo máximo de 10 años.

El citado registro, así como los tratamientos realizados por los intervinientes en la tramitación de las comunicaciones a través del Sistema Interno de Información, cumplirá con las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad de los datos personales adecuado al riesgo y, en su caso, aquellas previstas por la normativa sobre protección de datos que resulte de aplicación.

Por lo que se refiere a la información comprendida bajo el registro, la misma se mantendrá actualizada en todo momento, e incluirá los siguientes datos:

- Fecha de recepción de la comunicación.

Medio a través del cual ha sido recibida la comunicación.

- Datos de los interesados
- Resumen de la naturaleza de la comunicación
- Resumen de los hechos
- Fechas de información a los interesados
- Documentación
- Estado de la investigación

Los datos de carácter personal obtenidos en el marco de la investigación interna serán suprimidos cuando dejen de ser necesarios y pertinentes y, en todo caso, siempre que la comunicación haya resultado archivada, anterior o posteriormente a la investigación.

9. GARANTÍAS Y MEDIDAS DE PROTECCIÓN

9.1 Confidencialidad.

Grupo Solutia garantizará la máxima confidencialidad de las comunicaciones recibidas a través del Sistema Interno de Información, así como de la identidad del interesado.

Todas las personas que, siempre que sea estrictamente necesario para la adecuada gestión de la comunicación, tengan conocimiento de la misma, estarán obligadas a mantener rigurosamente la confidencialidad de las comunicaciones en todos sus extremos, incluyendo los datos de los interesados en el proceso y cualquier parte interviniente en el mismo.

Dicha obligación de confidencialidad no será de aplicación cuando sea necesario revelar o poner a disposición información y/o documentación relativa a las actuaciones del Compliance Officer, incluida la identidad de las personas implicadas, a requerimiento de la autoridad judicial o administrativa competente.

9.2 Garantía de indemnidad y presunción de inocencia.

Queda estrictamente prohibido adoptar represalias contra cualquier persona que, de buena fe, ponga en conocimiento de **Grupo Solutia**, a través del Sistema Interno de Información, incumplimientos del Código Ético, o cualquier otra normativa de **Grupo Solutia**, o que tenga consecuencias legales para la compañía. Si el Compliance Officer confirma que algún interesado que actúa de buena fe ha sido objeto de medida sancionadora o represalia, los autores o responsables serán objeto de investigación.

Grupo Solutia garantizará la protección adecuada de la intimidad y de los datos personales y la preservación del honor, la presunción de inocencia y el derecho de defensa, en especial, en los supuestos de comunicaciones infundadas, falsas o de mala fe, frente a las que se adoptarán las medidas disciplinarias que correspondan.

9.3 Transparencia en el uso de datos personales.

Grupo Solutia garantiza la aplicación del principio de transparencia en relación con el uso de datos personales en el Sistema Interno de Información, a través de la información facilitada a los interesados en el Anexo I- Información sobre el uso de datos personales de interesados.

ANEXO I. INFORMACIÓN SOBRE EL USO DE DATOS PERSONALES

1. Corresponsables del tratamiento y contacto del delegado de protección de datos.

De conformidad con la normativa de protección de datos de carácter personal, es considerado responsables del tratamiento **Grupo Solutia Tecnología S.L.**

Los Interesados pueden ponerse en contacto con **Grupo Solutia** a través del delegado de protección de datos: dpo@ascendiarc.com.

2. Categorías de datos personales.

Se podrán recabar las siguientes categorías de información en el marco de una Comunicación:

- Datos identificativos, tales como nombre y apellidos, datos de contacto y los datos relativos a la condición de empleado, tales como cargo o número de empleado, de los Interesados.
- Relación con **Grupo Solutia**.
- Incumplimientos comunicados.
- Documentación que pruebe los incumplimientos denunciados.

3. Fines y bases legales del tratamiento.

Los datos serán tratados a los efectos de detectar, investigar y evaluar legalmente las sospechas de incumplimiento de obligaciones laborales, comerciales o profesionales de acuerdo con su contrato, lo que incluye el incumplimiento del Código Ético, y cualquier otra normativa interna de **Grupo Solutia**.

Los hechos o actuaciones comunicados necesariamente tendrán que tener una vinculación efectiva con la relación laboral, comercial o profesional que vincule a los interesados con **Grupo Solutia**.

Asimismo, el tratamiento de los datos de carácter personal facilitados en la comunicación se establece en el marco de la relación laboral, comercial o profesional con **Grupo Solutia** con quien haya suscrito el contrato laboral, acuerdo comercial o profesional que corresponda. Por tanto, la base de legitimación para el tratamiento de los datos personales será, en algunos casos, la existencia de un interés público en prevenir y actuar frente a infracciones de la legislación aplicable y, en otros supuestos, la relación contractual o el interés legítimo que **Grupo Solutia** tiene en perseguir y prevenir acciones que contravengan las mencionadas políticas de **Grupo Solutia**.

4. Datos de los denunciados.

Asimismo, en cumplimiento de la normativa vigente, los Interesados serán informados del incumplimiento del que se les acusa, de los departamentos y terceros a quienes se puede ceder dicha información y de cómo ejercitar sus derechos con respecto a sus datos personales, de conformidad con la normativa de protección de datos. En cualquier caso, el ejercicio del derecho de acceso de los Interesados estará limitado a sus propios datos de carácter personal.

En todo caso, el plazo para informar a los Interesados no podrá exceder de un (1) mes desde la recepción de la comunicación, siempre que ello no obstruya la correcta investigación de los hechos comunicados o de otra forma las circunstancias alrededor de la comunicación no lo permitan, en cuyo caso la información se podrá aplazar hasta que el riesgo desaparezca.

5. Periodo de conservación.

Los datos personales recabados a través del Sistema Interno de Información se conservarán de conformidad con lo dispuesto en la legislación aplicable, tal y como se describe bajo el punto 8 del presente procedimiento. En concreto, los datos se conservarán únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos comunicados, que podrá prolongarse durante un máximo de tres (3) meses desde el registro de la comunicación. Sin embargo, en caso de que fuese necesario tratar los datos personales durante más tiempo para continuar la investigación o porque se decida entablar acciones legales, los datos se conservarán, en un entorno diferente al Sistema Interno de Información, en tanto sea necesario para concluir la investigación o para el ejercicio de acciones por parte de **Grupo Solutia** en los procedimientos judiciales correspondientes.

6. Destinatarios de los datos personales.

Para cumplir con las finalidades del tratamiento arriba señaladas, **Grupo Solutia** dará acceso a los datos personales a (i) prestadores de servicio, tales como asesores y colaboradores externos que presten soporte en la gestión o, en su caso, investigación de las comunicaciones recibidas a través del Sistema Interno de Información, y (ii) potencialmente, en caso de que sea necesario llevar a cabo medidas de actuación como consecuencia de la investigación, a aquellas áreas/departamentos/entidades de **Grupo Solutia** relevantes de cara a la investigación y las posibles medidas a tomar con respecto a la conducta comunicada en cuestión.

Igualmente, los datos podrán ser objeto de cesión a los Jueces y Tribunales, al Ministerio Fiscal o a las Administraciones Públicas competentes como consecuencia de la investigación que se pueda poner en marcha.

7. Derechos.

Por otro lado, se informa al Interesado de que, bajo las condiciones que se establecen en la normativa aplicable, podrá ejercitar los siguientes derechos:

- Derecho de acceso: tiene derecho a solicitar de **Grupo Solutia** que confirme si está tratando sus datos personales y, en caso afirmativo, a solicitar el acceso a los mismos. Los datos de acceso incluyen, entre otros, las finalidades del tratamiento, las categorías de los datos personales afectados, y los destinatarios o las categorías de destinatarios a los que los datos personales han sido o serán comunicados. Podrá obtener una copia de los datos personales que estén siendo objeto de tratamiento.
- Derecho de rectificación: Tiene derecho a solicitar a **Grupo Solutia** que rectifique los datos personales incorrectos o incompletos.
- Derecho de supresión (derecho al olvido): Tiene derecho a solicitar a **Grupo Solutia** que elimine sus datos personales.
- Derecho de limitación del tratamiento: Tiene derecho a solicitar la limitación del tratamiento de sus datos personales, si bien **Grupo Solutia** llevará a cabo un análisis caso por caso para determinar si efectivamente procede el ejercicio de dicho derecho.
- Derecho de oposición: Cuando se cumplan determinadas circunstancias, tendrá derecho a oponerse al tratamiento que realizamos de sus datos personales.

El Responsable del Tratamiento ha acordado que los Interesados podrán ejercitar sus derechos a la siguiente dirección: dpo@ascendiarc.com. Asimismo, tendrán el derecho a presentar una reclamación ante la autoridad de protección de datos competente en cada caso.

Documento original firmado digitalmente por el Presidente de Grupo Solutia, Valentín Rangel Enríquez, a fecha 23 de abril de 2024.