



POLÍTICA DEL SISTEMA INTERNO DE INFORMACIÓN

ÍNDICE

1. INTRODUCCIÓN	3
2. OBJETO Y ÁMBITO DE APLICACIÓN	3
3. PRINCIPIOS Y GARANTÍAS DEL SISTEMA INTERNO DE INFORMACIÓN	4
3.1. Buena fe y veracidad	4
3.2. Deber de colaboración.....	4
3.3. Confidencialidad y anonimato	4
3.4. Ausencia de represalias.....	5
3.5. Presunción de inocencia y derecho a la defensa.....	5
3.6. Imparcialidad	6
3.7. Protección de datos personales.....	6
4. COMISIÓN RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN.....	7
5. EL CANAL COMO PRINCIPAL HERRAMIENTA DEL SISTEMA INTERNO DE INFORMACIÓN	8
5.1. Identificación.....	8
5.2. Características y uso del Canal.....	8
6. CANAL EXTERNO.....	9
7. PRESENTACIÓN DE LA INFORMACIÓN	9
8. PROCEDIMIENTO DE GESTIÓN DE LA INFORMACIÓN.....	10
8.1. Acuse de recibo	10
8.2. Trámite de admisión	10
8.3. Fase de instrucción o investigación.....	11
8.4. Medidas preventivas	12
8.5. Resolución y terminación del expediente.....	12
8.6. Comunicación al Ministerio Fiscal u otra autoridad competente	13
9. REGISTRO DE INFORMACIONES.....	13
10. APROBACIÓN, PUBLICACIÓN, MODIFICACIÓN Y VIGENCIA	14
ANEXO I – DEFINICIONES	15
ANEXO II - MIEMBROS DE LA COMISIÓN RESPONSABLE DEL SISTEMA	16



1. INTRODUCCIÓN

El Sistema Interno de Información es una de las principales herramientas para asegurar el cumplimiento de la legalidad y evitar así la comisión de delitos e infracciones administrativas en el marco nacional y de la Unión Europea.

En este sentido, el Sistema Interno de Información se erige como uno de los pilares principales del compromiso del Grupo con los principios de cumplimiento normativo, ética y transparencia.

Por otro lado, el Canal se configura como la principal herramienta del Sistema Interno de Información y como el cauce preferente para informar sobre los delitos o infracciones administrativas graves y muy graves que puedan ocasionarse en el seno del Grupo.

2. OBJETO Y ÁMBITO DE APLICACIÓN

La presente Política regula y enuncia los principios generales del Sistema Interno de Información y constituye la guía principal para el uso del mismo (incluido el uso del Canal), definiéndose también las pautas, el protocolo de actuación y el procedimiento de gestión de la información recibida. Asimismo, la Política también tiene por finalidad otorgar medidas de protección y garantías a favor de los informantes y prohibir cualquier tipo de represalia contra ellos.

La presente Política es de aplicación, por un lado, a todas las empresas que forman CLUE y, por otro, a las siguientes personas (quienes podrán hacer uso del Sistema Interno de Información siempre que hayan obtenido la información sobre las infracciones en un contexto laboral o profesional):

- Socios, accionistas, administradores, apoderados, directivos, gerentes y empleados de CLUE, incluyendo personal en prácticas o formación.
- Terceros relacionados con o interesados en CLUE (“*stakeholders*”), incluidos, sin limitación, proveedores, clientes, colaboradores, candidatos a vacantes, etc.

El ámbito de aplicación material del Sistema Interno de Información y, por ende, la protección otorgada por la presente Política, se circunscribe a las informaciones relacionadas con acciones u omisiones que puedan ser constitutivas de: a) infracciones del Derecho de la Unión Europea incluidas en el artículo 2.a) de la Ley Reguladora del Sistema Interno de Información; b) infracciones penales o infracciones administrativas graves o muy graves; y c) infracciones del Código Ético de Clue.



3. PRINCIPIOS Y GARANTÍAS DEL SISTEMA INTERNO DE INFORMACIÓN

3.1. Buena fe y veracidad

De conformidad con lo dispuesto en la Ley Reguladora del Sistema Interno de Información, deberá atenderse a la buena fe en el uso de este y, en consecuencia, la presentación de comunicaciones a través del Sistema Interno de Información (incluido el Canal) deberá basarse en la creencia fundamentada o razonable de que se han producido o pueden producirse hechos que puedan ser constitutivos de las infracciones incluidas en el ámbito de aplicación material de la presente Política.

En este sentido, cualquier información comunicada por medio del Canal (o cualquier otro medio del Sistema Interno de Información) debe atender al principio de veracidad, no encontrándose protegida la remisión de informaciones falsas, fraudulentas o tergiversadas. Igualmente, debe evitarse basar cualquier comunicación en meras conjeturas, sospechas o rumores carentes de cualquier tipo de constatación o base.

No obstante, lo dispuesto en el párrafo anterior no debe entenderse como que la presentación de pruebas o evidencias sea un requisito inexcusable para el uso del Sistema Interno de Información, siendo que tendrán derecho a protección todas aquellas personas que tengan motivos razonables para pensar que la información es veraz en el momento de la comunicación o revelación, aun cuando no aporten pruebas concluyentes.

3.2. Deber de colaboración

Todas las personas, físicas o jurídicas incluidas en el ámbito de aplicación subjetivo recogido en el anterior apartado 2 tienen la obligación de informar sobre aquellas conductas que puedan ser constitutivas de las infracciones incluidas en el ámbito de aplicación material de la presente Política. Se deja constancia de que la comunicación podrá llevarse a cabo por el Canal o por cualquier otro medio previsto por la Ley Reguladora del Sistema Interno de Información (ej. canal externo).

3.3. Confidencialidad y anonimato

Se garantiza en todo momento el secreto y la confidencialidad de la identidad del informante, de la gestión del Sistema Interno de Información y, en general, de cualquier información que se contenga en la comunicación (incluida la identidad del presunto infractor y los hechos y omisiones que se le atribuyen).

En este sentido, solo podrán acceder al contenido de las comunicaciones tramitadas a través del Canal los miembros de la Comisión Responsable del Sistema, figura que es



objeto de regulación en el apartado 4 de la presente Política, así como en la Ley Reguladora del Sistema Interno de Información (Responsable del Sistema Interno de Información).

Nunca se revelará la identidad del informante sin su consentimiento expreso, a menos que tal identidad sea requerida por un órgano judicial o autoridad administrativa competente en la materia, en cuyo caso se comunicaría al informante salvo que dicha notificación pudiera comprometer la investigación o procedimiento judicial.

Adicionalmente a todo lo anterior, se permite la presentación de comunicaciones **anónimas**, lo cual aparecerá en el Canal como una casilla opcional al presentar la comunicación.

3.4. Ausencia de represalias

Se prohíbe terminantemente la adopción, tentativa de adopción o amenaza de cualesquiera represalias contra los informantes (incluidos aquellos que hayan realizado una revelación pública de conformidad con lo dispuesto en el Título V de la Ley Reguladora del Sistema Interno de Información) y terceros relacionados con este (mencionados en el artículo 3.4. de la Ley Reguladora del Sistema Interno de Información), siempre que hayan respetado las disposiciones de la Ley Reguladora del Sistema Interno de Información y de la presente Política. En cuanto a la definición de represalia, la Política se remite al artículo 36 de la Ley Reguladora del Sistema Interno de Información.

Cualquiera de estas personas que considere estar siendo objeto de cualquier represalia, tendrá derecho a dirigirse a cualquiera de los miembros de la Comisión Responsable del Sistema y solicitar amparo, información, asesoramiento y asistencia. Constatada la existencia de cualquier tipo de represalia (incluidas amenazas y tentativas de represalia) contra estas personas, se adoptarán las medidas correctoras o de protección necesarias. Igualmente, se deja constancia de que, tal y como se recoge en el artículo 36 de la Ley Reguladora del Sistema Interno de Información, cualquier persona que considere no haber sido objeto de protección por el Grupo frente a represalias, podrá solicitar la protección ante la autoridad competente.

3.5. Presunción de inocencia y derecho a la defensa

Se garantiza la presunción de inocencia y el derecho al honor de las personas afectadas por las comunicaciones que se cursen a través del Sistema Interno de Información.

Igualmente, tal y como se recoge en el artículo 39 de la Ley Reguladora del Sistema Interno de Información, las personas afectadas tendrán derecho a la defensa y al acceso



al expediente (respetándose en todo momento la confidencialidad de la identidad del informante). Además, se garantiza la confidencialidad de la identidad de las personas afectadas y de los hechos que se le atribuyen.

3.6. Imparcialidad

Se garantiza la imparcialidad de todos los miembros de la Comisión Responsable del Sistema. Dado que todos los miembros de la Comisión reciben la comunicación, si cualquiera de ellos estuviera en conflicto de interés quedaría recusado por el resto, quienes asumirían la labor de investigación y posterior resolución.

Se considera que los miembros de la Comisión Responsable del Sistema estarán en **“Conflicto de Interés”** en las siguientes situaciones:

- I. Ser la persona afectada por la comunicación.
- II. Existencia de vínculo familiar o análoga relación de afectividad con la persona afectada por la comunicación.
- III. Existencia de dependencia jerárquica directa respecto de la persona afectada por la comunicación.

3.7. Protección de datos personales

Se garantiza la protección de los datos personales incluidos en cualquier información remitida a través del Sistema Interno de Información, ateniéndose cualquier tratamiento de datos personales a lo dispuesto por la legislación y normativa aplicable en la materia.

Se deja constancia de que los datos personales facilitados a través del Sistema Interno de Información solo serán tratados para la investigación, gestión y resolución de las comunicaciones y, con ello, para cumplir con las obligaciones legales que afecten al Grupo como consecuencia de la Ley Reguladora del Sistema Interno de Información y demás normativa aplicable. En este sentido, se deja constancia de que la base legitimadora del tratamiento de los datos personales recae en la prevención de las infracciones penales y administrativas y en el cumplimiento de la legislación vigente.

Los datos facilitados serán recogidos y tratados por la sociedad matriz del Grupo, Clue Tech, S.A., como responsable del tratamiento.

Se deja constancia de que los datos solo serán conservados durante el tiempo imprescindible para la investigación de las comunicaciones recibidas y la resolución de los expedientes; no obstante, tal y como se recoge en la Ley Reguladora del Sistema Interno



de Información, se podrán conservar durante el tiempo necesario para dejar evidencia del cumplimiento de la legislación aplicable.

Por otro lado, cualquier información falsa será suprimida de inmediato, a excepción de que pudiera constituir una infracción penal, en cuyo caso se conservarán los datos durante el tiempo que dure el procedimiento penal. En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las infracciones, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de esta Política. Además, si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y su tratamiento.

Por último, se deja constancia de que el interesado podrá ejercitar cualesquiera de los derechos de acceso, rectificación, oposición, supresión, limitación del tratamiento, no ser objeto de tratamiento automatizado, portabilidad y retirar el consentimiento prestado, mediante comunicación por escrito a la dirección de correo electrónico hello@clue.aero.

4. COMISIÓN RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN

El responsable del correcto funcionamiento del Sistema Interno de Información será un órgano colegiado compuesto por tres (3) miembros, quienes han sido nombrados por el órgano de administración de la sociedad matriz de CLUE y cuyos datos se recogen en el **Anexo II** (la “**Comisión Responsable del Sistema**”). La Comisión Responsable del Sistema será el máximo responsable de la gestión y del correcto funcionamiento del mismo, tendrá la consideración de órgano colegiado Responsable del Sistema Interno de Información (a efectos del artículo 8 de la Ley Reguladora del Sistema Interno de Información) y será responsable de la implementación y tramitación diligente del procedimiento de gestión de informaciones. Todos los miembros de la Comisión Responsable del Sistema ejercerán sus cargos con independencia, autonomía y sin influencias de ningún otro órgano o persona del Grupo.

La Comisión Responsable del Sistema adoptará acuerdos por mayoría simple de sus miembros.

El nombramiento y/o cese de los miembros de la Comisión Responsable del Sistema será notificado a la Autoridad Independiente de Protección del Informante (o autoridad autonómica competente) dentro del plazo de diez (10) días hábiles siguientes al



nombramiento o cese. Igualmente, en el caso de cese deberán notificarse las razones que hayan justificado el mismo.

La Comisión Responsable del Sistema delegará en uno de sus miembros las facultades de gestión ordinaria de este (el “**Delegado**”).

5. EL CANAL COMO PRINCIPAL HERRAMIENTA DEL SISTEMA INTERNO DE INFORMACIÓN

5.1. Identificación

El Canal constituye el principal cauce para la recepción de comunicaciones en CLUE relativas a conductas incluidas en el ámbito de aplicación material de la presente Política. Este es accesible por cualquiera de las personas incluidas en el ámbito de aplicación personal de esta Política a través de la página web de CLUE (<https://clue-tech.personiowhistleblowing.com>).

La puesta en conocimiento de CLUE de cualquier información relativa a una posible infracción recogida en el ámbito de aplicación material de la presente Política deberá llevarse a cabo preferentemente a través del Canal, esto es, de la plataforma o enlace mencionado.

5.2. Características y uso del Canal

El Canal se ha desarrollado en atención a los principios de seguridad y preservación de la confidencialidad y el anonimato, de forma que solo los miembros de la Comisión Responsable del Sistema podrán acceder a la información comunicada a través del Canal.

Se deja constancia de que el uso del Canal se circunscribe a la comunicación de presuntas infracciones mencionadas en el apartado 2 de la presente Política, sin que el Canal pueda usarse para fines distintos.

El informante tendrá derecho a comunicar la información a través del Canal por escrito, tal y como indica la Ley Reguladora del Canal. Igualmente, el informante tendrá derecho a solicitar una reunión presencial con alguno de los miembros de la Comisión para presentar la información relativa a cualquier infracción incluida en el ámbito de aplicación material de la presente Política. En tal caso, la reunión deberá celebrarse dentro de los siete (7) días siguientes a la solicitud, salvo que no fuera posible por causas imputables al informante. En caso de reunión presencial, esta será grabada, previo consentimiento del informante, de conformidad con lo dispuesto en la Ley Reguladora del Sistema Interno de



Información. En caso de falta de consentimiento se deberá transcribir la conversación con el informante, quien deberá firmar y aceptar tal transcripción.

6. CANAL EXTERNO

Cualquier persona incluida dentro del ámbito de aplicación subjetivo de la presente Política, también podrá informar de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación material de esta Política ante la Oficina Andaluza contra el Fraude y la Corrupción (<https://buzon.antifraudeandalucia.es/#/>), ya sea directamente o tras haber cursado comunicación a través del Canal.

Se deja constancia de que el Canal es el cauce preferente para informar de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación material de esta Política, no obstante, cualquier persona podrá elegir, según las circunstancias, informar directamente a la Oficina Andaluza contra el Fraude y la Corrupción.

Este canal externo de información se regula en la Ley Reguladora del Sistema Interno de Información y en la web de la Oficina Andaluza contra el Fraude y la Corrupción, a las que se remite la presente Política.

7. PRESENTACIÓN DE LA INFORMACIÓN

La información deberá contener una descripción clara y detallada de las infracciones y, si fuera posible, identificar al autor y el lugar y fecha en que se produjeron. Asimismo, el informante podrá indicar cualesquiera indicios y elementos probatorios de los que se disponga y, en caso de documentación probatoria, podrá aportarla directamente a través del Canal.

Se deja constancia de que, a pesar de desconocer la identidad del autor, podrá aportarse información a través del Canal relativa a infracciones incluidas en el ámbito de aplicación material de la presente Política, en cuyo caso deberá indicarse el área o departamento en el seno del cual se ha cometido la infracción.

El informante podrá optar por incluir su identidad o, por el contrario, mantenerse en el anonimato. En caso de revelar su identidad, el informante podrá indicar uno o varios medios y direcciones de comunicación preferente (domicilio, correo electrónico, etc.), en cuyo caso se entenderá aceptada por su parte la posibilidad de que el Delegado u otros miembros de la Comisión Responsable del Sistema mantengan comunicaciones con él, a efectos de solicitar más información, aclaraciones e incluso reuniones.



Se deja constancia de que todos los datos aportados en la comunicación serán preservados en estricta confidencialidad y tratados conforme a las disposiciones sobre protección de datos personales incluidas en la Ley Reguladora del Sistema Interno de Información o en la presente Política.

Una vez reciba la comunicación, el informante recibirá un código único para acceder al Canal y consultar el estado de tramitación del asunto. Igualmente, de esta forma, en caso de haber solicitado preservar su anonimato, el informante podrá aportar nueva información sin necesidad de desvelar su identidad. Por motivos de seguridad, el informante nunca debe olvidar o perder el código único, puesto que no será posible recuperar el mismo.

8. PROCEDIMIENTO DE GESTIÓN DE LA INFORMACIÓN

8.1. Acuse de recibo

Se enviará al informante, en el plazo de siete (7) días naturales desde la comunicación, una notificación de acuse de recibo, salvo que ello pudiera poner en peligro la confidencialidad de la comunicación o que el informante hubiera decidido permanecer en el anonimato. No obstante, en cualquier caso, el acuse de recibo de la información será emitido y quedará registrado en el Canal, de forma que el informante que hubiera decidido permanecer anónimo podrá comprobar que se ha recibido la comunicación mediante el acceso al Canal con el código único.

8.2. Trámite de admisión

En el plazo de quince (15) días naturales desde la comunicación se notificará al informante (siempre que haya indicado algún medio de comunicación) acerca de la admisión o inadmisión a trámite de la comunicación. En caso contrario, se registrará la actuación en el Canal, de forma que el informante podrá comprobar el estado de tramitación del asunto mediante el acceso al Canal con el código único.

Corresponderá al decidir sobre la admisión o inadmisión a trámite de las comunicaciones que se reciban a través del Canal. Solo se inadmitirán a trámite comunicaciones en caso de que:

- Los hechos relatados carezcan de toda verosimilitud.
- Los hechos relatados no sean constitutivos de infracción incluida en el ámbito de aplicación material de la presente Política.

- La comunicación no se lleve a cabo por persona incluida en el ámbito de aplicación subjetivo de la presente Política.
- La comunicación carezca manifiestamente de fundamento.
- La comunicación verse sobre asuntos investigados en procedimientos anteriores, a menos que se aporte información nueva y relevante o que se den nuevas circunstancias de hecho de Derecho que justifiquen la investigación.

Para la inadmisión a trámite será necesaria la decisión mayoritaria de los miembros de la Comisión; se notificará al informante (o pondrá a su disposición a través del Canal) la decisión de inadmitir la comunicación y los motivos que justifiquen tal decisión.

Si la comunicación se refiere a hechos que ya están siendo investigados en otro expediente en curso, su tramitación e investigación se acumulará al expediente en curso.

8.3. Fase de instrucción o investigación

Una vez admitida a trámite la comunicación, se practicarán todas las diligencias de investigación oportunas para comprobar la veracidad de los hechos u omisiones relatados en la comunicación.

Las diligencias de investigación deberán ser proporcionales, necesarias y esenciales para cumplir con su finalidad. En este sentido, solo se obtendrán y almacenarán aquellos datos e informaciones que sean estrictamente necesarios para comprobar si se ha cometido o no alguna de las infracciones recogidas en el apartado 2 de la presente Política.

Se dará audiencia al informante (en caso de que haya informado acerca de medios de comunicación preferente) y, en su caso, a aquellos testigos que desee presentar el informante y que pudieran tener conocimiento de los hechos u omisiones objeto de la investigación.

Igualmente, se dará audiencia a la persona afectada por la comunicación; para ello, se le comunicarán las supuestas infracciones incluidas en la comunicación, momento desde el cual podrá presentar alegaciones por escrito. Igualmente la persona afectada podrá aportar aquellos medios de prueba que considere adecuados y pertinentes.

Todas las pruebas presentadas por las partes quedarán incorporadas al expediente. Se levantará acta de las declaraciones de las partes y testigos y también quedarán

incorporadas al expediente, previa firma de la parte o testigo concreto. Toda esta documentación quedará almacenada en el Sistema Interno de Información, en estricto cumplimiento de las obligaciones de confidencialidad.

La fase de instrucción o investigación no deberá superar los dos (2) meses desde la recepción de la comunicación, salvo casos de especial complejidad que requiera una ampliación del plazo, en cuyo caso la fase de instrucción o investigación podrá extenderse hasta los cuatro (4) meses y quince (15) días naturales desde la recepción de la comunicación.

Una vez finalizada la fase de instrucción o investigación, la Comisión Responsable del Sistema elaborará un informe en el que se establezca la propuesta de actuación a seguir para la terminación del expediente iniciado y la propuesta de sanción o archivo.

8.4. Medidas preventivas

Sin perjuicio de la presunción de inocencia y del resto de principios que inspiran la presente Política (resaltándose el principio de proporcionalidad), la Comisión Responsable del Sistema podrá decidir sobre la adopción de medidas preventivas dirigidas a evitar o prevenir los siguientes riesgos:

- I. Comisión de nuevas infracciones o continuidad en la conducta infractora.
- II. Ocultación o destrucción de medios de prueba.

8.5. Resolución y terminación del expediente

La Comisión Responsable del Sistema, una vez analizada la documentación del expediente, adoptará una de las siguientes conclusiones:

1. Archivar el expediente por considerar que los hechos u omisiones informadas no han quedado probados o que estos no pueden subsumirse en ninguna infracción recogida en el ámbito de aplicación material de la presente Política.
2. Declarar la existencia de infracciones y, en su caso, comunicar la resolución del expediente al órgano competente para establecer las medidas correctoras y adoptar las medidas disciplinarias o sanciones.

Dentro del plazo de tres (3) meses desde la recepción de la comunicación, se notificará al informante, o se pondrá a su disposición a través del Canal, las actuaciones realizadas con el fin de comprobar la veracidad de los hechos comunicados y el resultado de la



investigación, así como la resolución del expediente. No obstante, en caso de especial complejidad tal notificación podrá demorarse hasta los seis (6) meses desde la recepción de la comunicación.

En aras de instaurar el cumplimiento normativo y la ética como cultura del Grupo, la Comisión Responsable del Sistema podrá adoptar medidas tendentes a evitar posibles reiteraciones de infracciones, tales como:

1. Promulgar normas internas y políticas corporativas.
2. Impartir formación específica.
3. Establecer sistemas de monitorización de riesgos.

Cualquier medida a adoptar se llevará a cabo con estricto respeto del principio de preservación de la confidencialidad establecido en la Ley Reguladora del Sistema Interno de Información y en la presente Política.

8.6. Comunicación al Ministerio Fiscal u otra autoridad competente

En caso de que los hechos pudieran ser indiciariamente constitutivos de delito, se remitirán inmediatamente la información recibida sobre los mismos al Ministerio Fiscal. Por otro lado, en caso de que los hechos pudieran afectar a los intereses financieros de la Unión Europea, se comunicará la información a la Fiscalía Europea.

9. REGISTRO DE INFORMACIONES

Existirá un libro-registro de las comunicaciones recibidas a través del Canal en el que se recogerán los siguientes datos:

- a) Fecha de recepción de la comunicación;
- b) Código de identificación;
- c) Actuaciones desarrolladas;
- d) Resolución y medidas adoptadas; y
- e) Fecha de cierre.

En todo momento se garantizará la confidencialidad de la información contenida en el libro-registro. Tal y como se recoge en la Ley Reguladora del Sistema Interno de Información, 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 al contenido del referido libro-registro.



Los datos personales relativos a las informaciones recibidas y a las investigaciones internas a que se refiere este apartado solo se conservarán durante el periodo que sea necesario y proporcionado a efectos de cumplir con la Ley Reguladora del Sistema Interno de Información y demás normativa aplicable. En ningún caso podrán conservarse los datos por un periodo superior a diez (10) años.

10. APROBACIÓN, PUBLICACIÓN, MODIFICACIÓN Y VIGENCIA

La presente Política ha sido aprobada por el órgano de administración de la sociedad matriz de CLUE con fecha **1 de noviembre de 2023**.

Cualquier modificación de la presente matriz deberá ser aprobada por el órgano de administración de la sociedad matriz de CLUE a propuesta de la Comisión Responsable del Sistema. En cualquier caso, se llevarán a cabo revisiones de la presente política por la Comisión Responsable del Sistema con carácter bianual y se propondrán modificaciones y actualizaciones, en su caso, al órgano de administración de la sociedad matriz de CLUE.

La presente política entrará en vigor el próximo día 1 de diciembre de 2023 y estará en vigor de forma indefinida hasta que se adopte cualquier modificación según lo dispuesto en la presente cláusula.



ANEXO I – DEFINICIONES

“**Sistema Interno de Información**” se referirá al conjunto de herramientas, políticas y procedimientos establecidos en CLUE y tendentes al establecimiento de un sistema que garantice la recepción segura y el tratamiento efectivo de las comunicaciones, así como la protección a favor de los informantes y terceros relacionados.

“**Canal**” se referirá al Canal Interno de Información de CLUE (principal herramienta del Sistema Interno de Información entendido como cauce para la recepción de comunicaciones).

“**CLUE**” o “**Grupo**” se referirá conjuntamente a Clue Tech, S.A., Clue Technologies, S.L.U. y Clue Aerospace, S.L.U.

“**Ley Reguladora del Sistema Interno de Información**” se referirá 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

“**Comisión Responsable del Sistema**” su definición se recoge en el apartado 4 de la Política.

“**Delegado**” su definición se recoge en el apartado 4 de la Política.



ANEXO II - MIEMBROS DE LA COMISIÓN RESPONSABLE DEL SISTEMA

El órgano de administración de Clue Tech, S.A. ha nombrado, en el día de hoy, como miembros de la Comisión Responsable del Sistema a las siguientes personas:

- **Ignacio Fernández Montes**, en calidad de CEO de CLUE.
- **María Pilar Malpartida Giménez-Reyna**, en calidad de responsable de Recursos Humanos de CLUE.
- **Pablo Liñán Aller**, en calidad de asesor legal de CLUE; actuando además como Delegado.