PROCEDIMIENTO DE GESTIÓN DE COMUNICACIONES DEL CANAL INTERNO DEINFORMACIÓN

Control de Versiones:

Revisión	Versión	Causa y detalle del cambio	Responsable	Fecha cambio/revisión	Fecha aprobación
2023	1.0	Creación del documento	Isabel Moreno	27/11/2023	28/11/2023

ÍNDICE

1. INTRODUCCIÓN

La "**Ley 2/2023, de 20 de febrero, reguladora de la protección de personas que informen sobre infracciones normativas y de lucha contra la corrupción"** (en adelante **Ley 2/2023**) ha transpuesto al ordenamiento jurídico español La Directiva europea 2019/1937 Directiva "Whistleblowing", relativa a la protección de las personas que informan sobre infracciones al Derecho de la Unión. Esta norma establece la obligatoriedad de que las entidades jurídicas de los sectores públicos y privados, con más de 50 empleados, y aquellas personas jurídicas del sector privado que entren en el ámbito de aplicación de los actos de la Unión europea en materia de servicios, productos y mercados financieros, dispongan de un **Sistema Interno de Información** (SII) para comunicar de manera oportuna, adecuada y confidencial, las acciones u omisiones previstas en esta Ley.

Este Sistema Interno de Información se configura como el cauce preferente para recibir información sobre aquellas acciones u omisiones que se identifican en la misma, y a estos efectos deberá:

- Permitir la comunicación sobre las infracciones previstas en la Ley.
- Garantizar la confidencialidad de la identidad de las personas que hagan uso del sistema de información, y de cualquier tercero mencionado en la comunicación realizada y de las actuaciones que se desarrollen en su gestión.
- Permitir la presentación de comunicaciones por escrito o verbalmente, o de ambos modos.
- Integrar los distintos canales internos de información que pudieran establecerse en la entidad.
- Garantizar la tramitación efectiva de las comunicaciones presentadas.
- Contar con un Responsable del Sistema.
- Contar con una Política y un Procedimiento de Gestión de las comunicaciones recibidas.
- Establecer las garantías para la protección de las personas informantes.

GSSecurity tiene implantada una **"Política del Sistema Interno de Información y Protección del Informante"** en la que se establecen los principios generales del Sistema Interno de Información, con los que se compromete en el desarrollo de la actividad empresarial de las empresas que lo integran. Esta Política recoge igualmente el "**Canal Interno de Información"** (en adelante "**Canal de Información"**) que se ha establecido como mecanismo de comunicación y conocimiento confidencial, transparente y adecuado para informar de aquellos comportamientos que puedan conllevar alguna irregularidad o de algún acto contrario a la legalidad, o a las normas de comportamiento del Código Ético y demás normas internas aplicables, cometidos por quienes integran las empresas GSSecurity, tanto de su equipo de dirección, como por las personas trabajadoras en general, así como por las personas representantes o trabajadoras de empresas que colaboran con el Grupo en sus distintas actividades..

Teniendo en cuenta todos estos antecedentes, se elabora el presente "**Procedimiento de Gestión de Comunicaciones del Canal Interno de Información"** (en adelante el "**Procedimiento"**), que desarrolla la Política antes mencionada, y se constituye como una herramienta corporativa puesta al servicio de todas las personas a quienes más adelante se identificará, para facilitar la comunicación, gestión, investigación, seguimiento, resolución, y confidencialidad de las comunicaciones realizadas de buena fe, en relación con posibles comportamientos o actuaciones contrarias a la legalidad vigente, y de igual manera, a los principios, normas éticas e internas GSSECURITY,y su consiguiente protección frente a cualquier tipo de represalia.

2. ALCANCE

Este Procedimiento es aplicable a las entidades que forman parte de GSSecurity. A estos efectos, tendrán la consideración de Grupo, la entidad matriz, y las filiales (aquellas entidades sobre las que ostenta el control) que a continuación se indican:

- GLOBAL SYSTEM SECURITY, S.L. B64446263
- GLOBAL SECURITY SOLUTIONS, S.L. B87093209

3. ÁMBITO DE APLICACIÓN

3.1 Ámbito Material

Todas las personas identificadas en el apartado siguiente tendrán la posibilidad de comunicar a través del Canal de Información habilitado por GSSecurity, aquellas acciones u omisiones que vulneren la legislación vigente, de acuerdo con lo establecido en la Política corporativa del Sistema Interno de Información.

Por consiguiente, podrán ser objeto de información, y serán tramitadas conforme a lo dispuesto en el presente Procedimiento, las comunicaciones que se encuentren relacionadas con:

1. Aquellas acciones u omisiones que puedan constituir **infracciones del Derecho de la Unión Europea**, descritas en la Ley 2/2023, de 20 de febrero, reguladora de la protección de personas que informen sobre infracciones normativas y de lucha contra la corrupción.
2. Aquellas acciones u omisiones que puedan ser **constitutivas de infracción penal (delito)**.

3. Acciones que puedan ser **constitutivas de infracción administrativa** grave o muy grave.

De igual manera, podrán ser objeto de comunicación a través del Canal de Información, aquellas informaciones que puedan implicar una violación de los principios y deberes que se contemplan en el Código Ético de GSSecurity.

El Canal de Información no puede ser utilizado como buzón de sugerencias, ni como medio para presentar consultas o solicitudes, quejas o reclamaciones. A título de ejemplo, no podrán comunicarse a través de este medio:

•Quejas o reclamaciones formuladas por asegurados sobre el contrato del seguro que tengan suscrito. Éstas deben ser interpuestas ante el Servicio de Atención al Cliente de la Entidad a través de los medios y canales establecidos a este efecto.

•Comentarios o juicios de valor subjetivos que no estén relacionados en modo alguno con una acción, conducta, o comportamiento contrario a la legalidad vigente, o poco ética.

3.2. Ámbito Subjetivo

Podrán hacer uso del Canal de Información las siguientes personas:

a) Personas que trabajen por cuenta ajena, empleadas en cualquiera de las sociedades del Grupo.

b) Personas que realicen trabajos por cuenta propia o autónomos.

c) Accionistas y personas pertenecientes al órgano de administración, dirección o supervisión de las empresas, incluidas aquellas que no tengan la condición de ejecutivas, así como el personal voluntario y en prácticas remuneradas o no; personas que ya no tengan relación con las empresas de GSSecurity por haber expirado ésta, personal en formación o becarios.

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

e) Personas que comuniquen o revelen públicamente información sobre infracciones obtenidas en el marco de una relación laboral ya finalizada.

f) Personas cuya relación laboral todavía no haya comenzado, si la información sobre la infracción que se comunique se obtiene durante el proceso de selección o negociación precontractual.

g) Todas aquellas personas que de forma directa o indirecta intervengan en el procedimiento y puedan ser represaliados por ello (asesores del Informante, representantes, etc.).

En adelante, las personas aquí mencionadas serán referidas como "**lo/s informante/s"** o "**persona/s informante/s".**

4. RESPONSABLE DEL SISTEMA DE INFORMACIÓN

El órgano de administración de la entidad matriz de GSSecurity será el competente para la designación de la persona física responsable de la gestión del sistema de información (en adelante el **"Responsable del Sistema"**), y su destitución o cese.

La persona Responsable del Sistema desarrollará sus funciones de forma independiente y autónoma respecto del resto de los órganos de las entidades de GSSecurity a quienes resulte de aplicación el presente Procedimiento. No podrá recibir instrucciones de ningún tipo en su ejercicio, y dispondrá de todos los medios personales y materiales necesarios para llevarlas a cabo.

Corresponde al Responsable del Sistema el seguimiento, cumplimiento y comprobación de la suficiencia de las medidas recogidas en el presente Procedimiento, así como la tramitación y gestión de las comunicaciones que se puedan realizar al amparo de lo establecido en este documento, garantizando en todo momento la confidencialidad en el tratamiento de dichas comunicaciones.

El Responsable del Sistema gestionará toda comunicación que se reciba a través del Canal de Información establecido, sobre la posible comisión de una actuación ilícita o irregular descritas en el apartado 3.1 del presente procedimiento.

5. CANAL DE INFORMACIÓN

GSSecurity ha habilitado el espacio "Canal del Informante" dentro de su página web **www.GSSecurity.es**donde se publicará la información sobre el canal interno para la comunicación de las informaciones sobre las acciones u omisiones recogidas en el apartado 3.1 anterior del Procedimiento, relacionadas con las actividades desarrolladas por las empresas GSSecurity.

En este canal se han integrado los diferentes canales internos ya existentes y que se encontraban habilitados para efectuar estas comunicaciones, en función de la naturaleza u origen de las mismas en el siguiente enlace:

https://compliance.legalsending.com/canal/?C=48601369019012376

Se trata de un canal seguro, con las garantías de confidencialidad, y protección del Informante.

La realización de una comunicación a través del Canal de Información, no impide que la persona informante pueda realizar esta misma comunicación ante cualquier otro organismo que resulte competente.

De igual manera, toda persona física podrá utilizar el canal externo de información de la Autoridad Independiente de Protección del Informante (A.A.I.) regulado en la Ley 2/2023, o de las autoridades u órganos autonómicos correspondientes que hubieran

establecido igualmente un canal de información general, o de cualquier otro organismo público nacional o europeo que tuviera un canal específico para comunicar la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación material de este Procedimiento, ya sea directamente o previa comunicación a través del canal interno.

6. RECEPCIÓN DE COMUNICACIONES

Cualquier persona informante que detecte una conducta susceptible de ser comunicada a través del Canal de Información habilitado por GSSECURITY, deberá ponerla en conocimiento del Responsable del Sistema a través de los siguientes medios:

- El envío de una comunicación a la dirección electrónica identificada en el apartado 5 anterior.
- El envío postal, dirigido a GSSECURITY, a/a Responsable Sistema Interno de Información, c/ Balanço i Boter 22, 1º3. 08302 Mataró.
- A solicitud de la persona informante, mediante petición dirigida al Responsable del Sistema, podrá realizarse la comunicación mediante una reunión presencial. En este caso, se advertirá a la persona informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo con lo que establecen el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales.

Las personas que efectúen una comunicación a través de los medios dispuestos en este Procedimiento, deberán garantizar que, en caso de facilitar datos personales éstos son verdaderos, exactos, completos y actualizados.

Las personas que presenten una comunicación informando sobre una irregularidad o incumplimiento de la normativa que resulte de aplicación, deben hacerlo de buena fe, con respeto a la verdad, con el convencimiento de actuar correctamente y solamente en beneficio de GSSECURITY, y de la sociedad en general.

Se entenderá que una comunicación ha sido realizada de buena fe, y conforme a cuanto se encuentra establecido en el presente Procedimiento, cuando:

- La información que se traslade esté basada en hechos o indicios de los que razonablemente pueda desprenderse que se ha cometido una acción u omisión contraria a la legalidad vigente.
- La comunicación se haya efectuado sin desprecio hacia la verdad, y sin ánimo de venganza, de acosar moralmente, de causar un perjuicio laboral o profesional, o de lesionar el honor de una persona o de un tercero.

El mal uso del Canal de Información, o la realización de comunicaciones falsas o de mala fe, podrá, cuando así corresponda y hayan quedado constatadas estas circunstancias, conllevar la imposición de una sanción disciplinaría por parte GSSECURITY, sin perjuicio de la posible responsabilidad civil, por la lesión al honor o la comisión de un delito de injurias o calumnias, que este tipo de comportamientos o actuaciones puedan conllevar.

GSSECURITY no permitirá que se tomen represalias de ningún tipo, contra las personas que efectúen las comunicaciones que hayan sido remitidas de buena fe. En este sentido las personas informantes estarán protegidas como más adelante se establece de forma expresa y tal y como se recoge en la Política del Sistema Interno de Información y Protección al Informante del Grupo.

7. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES

El Procedimiento regulado en este documento, comporta el almacenamiento de datos personales, por lo que las condiciones de su implantación están sometida a la legislación vigente, por consiguiente, todo tratamiento de datos personales realizado en aplicación del presente Procedimiento se realizará de conformidad con lo dispuesto en la Ley 2/2023, de 20 de febrero, reguladora de la protección de personas que informen sobre infracciones normativas y de lucha contra la corrupción, con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante RGPD), así como con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD).

De conformidad con lo establecido en la citada normativa, se informa que los datos personales que se proporcionen como consecuencia del presente Procedimiento serán tratados en calidad de responsable del tratamiento por el órgano de administración o de gobierno correspondiente de cada una de las empresas que forma parte GSSECURITY, y se encuentran citadas en el apartado 2 "Alcance" de este Procedimiento, con la finalidad de cursar, investigar y gestionar la comunicación recibida.

El tratamiento se ampara, tanto en el cumplimiento de la obligación legal que se establece en la Ley 2/2023, como en el interés público. Durante la tramitación del mismo se dará la información establecida en los artículos 13 y 14 del RGPD tanto a la persona informante como a la parte afectada

El acceso a los datos está limitado dentro de sus competencias y funciones, exclusivamente al Responsable del Sistema, a la persona responsable de Cumplimiento Normativo, y al Delegado de Protección de Datos.

GSSecurity tiene implementadas medidas de seguridad en el Canal del Informante y en los canales internos de información que están integrados en citado canal, que garantizan la máxima confidencialidad respecto de las comunicaciones realizadas, impiden el acceso a personal no autorizado, y las posibles pérdidas de dicha información.

En aras al principio de confidencialidad, la persona afectada por la comunicación remitida a través del Canal del Informante no podrá acceder ni a los datos de la persona que la hubiera efectuado, ni de cualquier persona que pueda estar implicada en las acciones u

omisiones comunicadas, durante la tramitación del procedimiento. El derecho de acceso de la persona afectada queda limitado, por tanto, a sus propios datos personales.

Los datos que sean objeto de tratamiento podrán conservarse en el Sistema Interno de información únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados. Este periodo no excederá en ningún caso de tres meses desde la recepción de la comunicación sin que se hubieren iniciado actuaciones de investigación, salvo que en el caso de que la finalidad sea la de dejar evidencia del funcionamiento del sistema o que se deriven procedimiento administrativos o judiciales.

Los interesados podrán ejercer sus derechos en materia de protección de datos mediante una comunicación escrita dirigida a la dirección postal: c/ Balanço i Boter 22, 1º3. 08302 Mataró, o en el correo electrónico lopd@GSSecurity.es, con identificación del asunto: "canal informante".

Puede consultar más información en nuestra política de privacidad del canal del informante que se encuentra en esta sección de las páginas web anteriormente indicadas.

8. DERECHOS Y DEBERES DE LA PERSONA INFORMANTE

8.1. Derechos de la persona informante:

- Derecho a la confidencialidad, de forma que el Responsable del Sistema no podrá comunicar a la persona afectada la identidad de la persona informante, con las excepciones legalmente previstas o en aquellos supuestos en los que este último lo consienta expresamente cuando, de lo contrario, no fuera posible proseguir con la investigación.
- Derecho a conocer la información relativa al tratamiento de datos personales en el marco del Sistema Interno de Información.
- Derecho a la información de la posible comunicación de los datos, al amparo de la normativa, tanto a jueces y Tribunales, como a las personas u organismos que se estimen pertinentes, implicadas en cualquier fase de la investigación.
- Derecho a que no se adopten represalias contra ella por razón de la comunicación efectuada, siempre que actúe de buena fe.
- Derecho a ser informada de la resolución o archivo de la comunicación realizada, en su caso.

8.2. Deberes de la persona informante:

- Deber de actuar de buena fe. Las comunicaciones realizadas de mala fe podrán dar lugar a las medidas disciplinarias y/o sancionadoras que en su caso procedan contra la persona denunciante.
- Deber de aportar los datos y documentos de los que disponga relacionados con los hechos comunicados.
- Deber de confidencialidad. La persona informante no podrá comunicar a ningún órgano o persona distintos del Responsable del Sistema la identidad de la persona afectada por la comunicación que lleve a cabo, con las excepciones legalmente previstas.

La conducta de la persona informante que actúe de buena fe y con voluntad de colaboración podrá ser tenida en cuenta por GSSECURITY al efecto de calificar o, ensu caso, sancionar su participación o relación con los hechos objeto de comunicación.

9. DERECHOS DE LA PERSONA AFECTADA

- Derecho a que se le comunique que se encuentra inmersa en un proceso de investigación, fruto de una comunicación presentada a través del Canal de Información, en el tiempo y forma que se resulte adecuado para garantizar el buen fin de la investigación de los hechos.
- Respeto a la presunción de inocencia.
- Derecho a recibir información sobre las acciones u omisiones que se le atribuyen

- Derecho a presentar alegaciones por escrito, a ser oído, y a aportar aquellos medios de prueba que considere adecuados y pertinentes.

10. REQUISITOS DE LAS COMUNICACIONES

Para que una comunicación realizada a través del Canal de Información, pueda ser gestionada de forma adecuada, en la medida de lo posible, deberá tener el siguiente contenido mínimo:

- Identificación de la persona informante: nombre y apellidos y datos de contacto (dirección de correo electrónico y/o teléfono), salvo que se trate de comunicaciones efectuadas de forma anónima.
- Identificación de la persona/s responsable/s de la irregularidad comunicada, en caso de ser conocidas.
- Irregularidad comunicada, debiendo describirse los hechos y motivos de la misma y especificar dónde y cuándo tuvieron lugar tales hechos, aportando evidencias y pruebas de los mismos, siempre que sea posible.

Se podrá contactar con la persona informante, en caso de que sea necesario, para que aporte información adicional a la comunicada.

En cumplimiento a lo establecido en la Ley 2/2023, se admitirán las **comunicaciones anónimas** si estas tienen cierto grado de verosimilitud. En este caso la persona Responsable del Sistema, actuará diligentemente en orden a comprobarla. También se admitirán si sirven para completar la información recibida en una comunicación previa que cumpla los requisitos mínimos mencionados.

Toda persona que efectúe una comunicación sobre una irregularidad o quebrantamiento de la legalidad vigente a través del Canal de Información debe de tener indicios racionales, que sustenten la misma, por lo que la comunicación deberá venir acompañada, cuando resulte posible, de las pruebas que acrediten los hechos, al menos indiciariamente. Cualquier prueba debe de haber sido obtenida por el informante de forma licita, es decir con respeto a la ley y los derechos y las garantías constitucionales.

Si al realizar la comunicación se hubiera incurrido en un defecto, en cuanto a la falta de información mínima necesaria, que sea subsanable, se concederá a la persona

informante, un plazo de cinco (5) días hábiles, para que subsane el defecto, advirtiéndole en este caso de que se procederá al archivo de la comunicación sin más trámite, si el defecto no es subsanado en este plazo.

11. RECEPCIÓN Y TRATAMIENTO DE LAS COMUNICACIONES

11.1 Registro

Recibida una comunicación a través del canal de información, el Responsable del Sistema procederá a su registro, siéndole asignado un código de identificación. Este registro contará con los niveles de protección adecuados para garantizar la seguridad de los datos incorporados y evitar su manipulación. El acceso a este registro estará restringido exclusivamente al Responsable del Sistema. En dicho registro quedarán documentadas todas las comunicaciones recibidas, cumplimentando los siguientes datos de cada una de ellas:

a) Código de identificación.

b) Fecha de recepción.

c) Naturaleza de la comunicación y personas involucradas.

d) Fecha de inadmisión, en su caso.

d) Estado de la investigación e instrucción.

e) Resolución del expediente.

f) Medidas adoptadas.

g) Fecha de cierre.

11.2 Acuse de recibo

En un plazo no superior a siete días hábiles desde dicha recepción se procederá a acusar recibo de la comunicación efectuada, a menos que el informante expresamente haya renunciado a recibir comunicaciones relativas a la investigación, o que el Responsable del Sistema considere razonablemente que el acuse de recibo de la información pudiese comprometer la protección de la identidad del informante, o que la comunicación se haya efectuado de forma anónima.

11.3 Comprobación

Registrada la comunicación, el Responsable del Sistema comprobará si aquella expone hechos o conductas que se encuentran dentro del ámbito de aplicación material recogido en el apartado 3.1 anterior.

En el supuesto de que el Responsable del Sistema comprobase que la comunicación recibida es pertinente, pero su contenido es insuficiente, incompleto o no proporciona

el detalle necesario para que se pueda iniciar la instrucción del expediente, se remitirá a la persona informante una comunicación solicitándole la aportación de información o documentación adicional en un plazo máximo de cinco (5) días hábiles, desde la recepción de dicha comunicación, salvo que se tratase de comunicaciones realizadas de forma anónima. Transcurrido dicho plazo sin contestación del informante en este sentido, se procederá al archivo del expediente.

Realizado este análisis preliminar, la persona Responsable del Sistema, decidirá, en un plazo que no podrá ser superior a cinco (5) días hábiles desde la fecha de entrada en el registro de la información:

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

1. Cuando la información trasladada carezca de toda verosimilitud, resulte falta de fundamento, notoriamente falsa o no tenga soporte probatorio alguno.

2. Cuando la información facilitada tenga carácter genérico y no se refiera a hechos o datos concretos contrastables.

3. Cuando los hechos relatados en la comunicación realizada no sean constitutivos de infracción del ordenamiento jurídico o de la normativa interna GSSECURITY, recogida en el apartado 3.1. de este Procedimiento.

4. Cuando la comunicación carezca manifiestamente de fundamento o existan, a juicio de la persona Responsable del Sistema, indicios racionales de haberse obtenido la información comunicada 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.

5. 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. En estos casos, el Responsable del Sistema, notificará la resolución de manera motivada.

6. Cuando respecto de los mismos hechos y conductas comunicadas se hayan realizado anteriormente actuaciones de investigación que se encuentren ya cerradas.

7. Cuando se trate de hechos y circunstancias que están siendo o hayan sido ya investigadas por la autoridad judicial, el Ministerio Fiscal o la policía judicial.

8. Cuando exista otra circunstancia justificada apreciada por el Responsable del Sistema.

La inadmisión se comunicará al informante dentro de los cinco (5) días hábiles siguientes, salvo que la comunicación fuera anónima o el informante hubiera renunciado a recibir comunicaciones del Responsable del Sistema, procediendo igualmente a la supresión de los datos personales recogidos en el registro de la comunicación realizada.

b) Admitir a trámite la comunicación: La admisión a trámite se comunicará al informante, salvo que la comunicación fuera anónima, o el informante hubiera renunciado a recibir comunicaciones del Responsable del Sistema.

c) Remitir con carácter inmediato la información al Ministerio Fiscal cuando los hechos comunicados 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.

11.4 Excepciones

Si la información que se traslada a través del canal interno de información se encuentra relacionada tanto con infracciones de la normativa sobre **blanqueo de capitales y financiación del terrorismo**, como con la normativa sobre la **distribución de seguros**, resultará de aplicación la normativa específica sobre comunicación de infracciones en dichas materias, tal y como se establece en la Ley 2/2023. Por consiguiente, el Responsable del Sistema comunicará al informante el medio a través del cual deberá realizarse la correspondiente comunicación.

12. INSTRUCCIÓN

Si del contenido de la comunicación realizada a través del Canal de Información, existieran indicios de la comisión de un incumplimiento legal o de alguna irregularidad, se iniciará la fase de instrucción del expediente abierto con respecto a dicha comunicación.

La instrucción comprenderá todas aquellas actuaciones adecuadas y pertinentes, y la práctica de las pruebas que se consideren necesarias, encaminadas al debido esclarecimiento y determinación de los hechos comunicados, y a la comprobación de su verosimilitud y materialización, entre las que se incluyen las siguientes:

- Investigar los hechos y recopilar las evidencias necesarias, que permitan sustentar los resultados de la investigación.
- Documentar las acciones realizadas.
- Cumplir con las exigencias de la normativa de protección de datos.
- Elaborar el informe final con el resultado de la instrucción.

En esta fase de Instrucción, se dará trámite de audiencia a la persona afectada, salvo que se ponga en peligro la capacidad para investigar o recopilar pruebas de manera eficaz por el riesgo de destrucción o alteración de las mismas por parte de dicha persona, en cuyo caso este trámite podrá retrasarse hasta un máximo de dos meses.

Así mismo, el trámite de audiencia se dará a los terceros que puedan actuar como testigos, cuya intervención tendrá carácter estrictamente confidencial.

*Si una comunicación recibida en el Canal de información se encuentra relacionada con el ámbito de competencia de la **Comisión de Actuación frente al Acoso**, el Responsable del Sistema de Información dará oportuno traslado de la misma a la citada Comisión para su completa tramitación y resolución, todo ello de acuerdo al "Protocolo

para la prevención y tratamiento del acoso moral, sexual o por razón de sexo" establecido a estos efectos. Esta Comisión informará al Responsable del Sistema del cierre de sus procedimientos para que éste pueda dejar constancia en su registro del cierre del expediente.

Si en cualquier momento de la instrucción se tuviese conocimiento de la existencia de actuaciones en curso en el ámbito judicial o administrativo por los mismos hechos, el Responsable del Sistema podrá acordar la suspensión de la actuación de instrucción que se esté llevando a cabo, y reanudarla si hubiera aspectos relevantes no decididos en aquellos ámbitos.

Conflicto de interés: En ningún caso una persona podrá participar, ni directa ni indirectamente, en la instrucción (tramitación e investigación) de una comunicación que le afecte, quedando excluida de la gestión/instrucción de la comunicación, quedando bloqueado su acceso a cualquier actuación relacionada con la misma. Igualmente, tampoco podrán participar personas que dependan jerárquicamente de la afectada, ni personas de las que la persona afectada dependa jerárquicamente.

13. RESOLUCIÓN

Concluidas todas las actuaciones desarrolladas en la fase de instrucción del expediente, se elaborará un Informe, que, al menos, tendrá los siguientes contenidos:

a) Una exposición sucinta de los hechos relatados, la fecha de registro, y el código interno asignado para la identificación de la comunicación.

b) Las actuaciones realizadas con el fin de comprobar la veracidad de los hechos comunicados.

c) Las conclusiones alcanzadas en la instrucción y la valoración de las diligencias y de los indicios que las sustentan, dejando igualmente constancia de las recomendaciones que se considere oportuno realizar.

La persona Responsable del Sistema, de acuerdo con el contenido de este informe, adoptará alguna de las siguientes decisiones:

a) **Archivo del expediente**, que será notificado al informante y, en su caso, a la persona afectada. El informante tendrá derecho a la protección prevista en la Ley 2/2023, de 20 de febrero, reguladora de la protección de personas que informen sobre infracciones normativas y de lucha contra la corrupción, salvo que, como consecuencia de las actuaciones llevadas a cabo en fase de instrucción, se concluyera que la comunicación a la vista de la información recabada debía haber sido inadmitida por concurrir alguna de las causas previstas en el apartado 11.3 de este Procedimiento.

b) **Remisión al Ministerio Fiscal** si, pese a no apreciar inicialmente indicios de que los hechos comunicados 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.

c) **Traslado** a la Dirección de la entidad matriz GSSecurity, para la aplicación de las medidas de corrección y/o, en su caso, disciplinarias que pudieran corresponder, si de las actuaciones realizadas se concluye que un integrante de las empresas GSSecurity ha llevado a cabo una **conducta irregular o ilícita**, incumpliendo la normativa interna o externa de obligado cumplimiento.

Si la implicación en los hechos comunicados y finalmente probados fuese de un Socio de Negocio, proveedor de mercancías, servicios y/o suministros, el Responsable del Sistema dará traslado al Departamento o Área de las empresas GSSecurity que haya realizado la contratación o que sea responsable del cumplimiento de sus compromisos, para la adopción de las medidas que se consideren adecuadas.

Cuando del contenido de la comunicación o de la instrucción de la misma se ponga de manifiesto la posible existencia de responsabilidades penales relevantes que puedan afectar a la cualquiera de las empresas GSSecurity, el Responsable del Sistema informará de inmediato al Consejo de Administración correspondiente, a través de la Comisión de Auditoría y Cumplimiento Normativo si existiese, y al Director del departamento de Asesoría Jurídica.

En el caso de que se compruebe que una comunicación ha sido realizada infringiendo la buena fe contractual, proporcionando información sobre hechos y/datos falsos o tergiversados por una persona integrante GSSecurity, tal extremo se pondrá de manifiesto a la persona responsable de la Dirección de la entidad matriz GSSecurity, para que se adopten, en su caso, las medidas disciplinarias queresulten pertinentes.

El plazo para la tramitación del expediente, finalizar las actuaciones, y dar respuesta al informante, en su caso, no podrá ser superior a tres meses desde la entrada en registro de la información, salvo aquellos casos de especial complejidad que requieran una ampliación del plazo indicado, el cual podrá extenderse hasta un máximo de otros tres meses adicionales. Cualquiera que sea la decisión, se comunicará al informante, salvo que haya renunciado a ello o que la comunicación sea anónima.

14. INFORME SOBRE EL CANAL INTERNO DE INFORMACIÓN

De forma periódica, y como mínimo una vez al año, el Responsable del Sistema informará al Consejo de Administración de las empresas GSSecurity, sobreel número de comunicaciones presentadas, tramitadas y archivadas, la tipología de las mismas, así como de la necesidad de adopción de medidas adicionales o complementarias, a fin de mejorar en su caso, la gestión del procedimiento. Esta información será analizada y valorada con el objeto de mejorar las medidas tendentes aprevenir cualquier incumplimiento de la normativa que resulte de aplicación, así como para mitigar el riesgo de que puedan llegar a cometerse los delitos e infracciones recogidos en el Modelo interno para la Prevención de Riesgos Penales que pudieran cometerse con los medios o bajo la cobertura GSSecurity.

Sin perjuicio de lo anterior, de forma extraordinaria, informará a la Dirección General de las empresas GSSecurity y a sus Consejos de Administración, cuando existan circunstancias que así lo requieran.

15. DIVULGACIÓN Y FORMACIÓN SOBRE EL CANAL INTERNO DE INFORMACIÓN

Con el objetivo de que el Sistema Interno de Información y el Canal de Información sean efectivos, su existencia se pondrá en conocimiento de todo el personal de las empresas GSSecurity a través de un comunicado interno en el que se indique la forma de acceder al mismo y los trámites del procedimiento.

En todo caso, esta información se mantendrá publicada de forma permanente en la Intranet de las empresas GSSecurity.

En dicha información se harán constar necesariamente los siguientes aspectos:

- Uso del Canal Interno de Información.
- Principios generales del procedimiento de gestión de las comunicaciones.
- La confidencialidad de las comunicaciones recibidas.
- La protección de la persona informante, haciendo saber que la empresa garantizará que no se tome ningún tipo de represalia contra las personas que informen sobre la comisión de irregularidades, exceptuándose exclusivamente aquellos supuestos en los que quede acreditada la mala fe de la persona informante, pudiendo adoptarse en este caso las medidas sancionadoras que legalmente correspondan.
- El tratamiento de datos personales en el marco del Sistema Interno de Información.

16. ACTUALIZACIÓN DEL PROCEDIMIENTO Y VIGENCIA

Este Procedimiento deberá revisarse, y si fuese necesario actualizarse, como mínimo una vez al año, y cuando sea necesario ante cambios materiales en el contenido del mismo, debiendo quedar registro de cada proceso de actualización, los motivos de ésta y los cambios realizados.

La responsabilidad de dicha revisión y actualización recaerá en el Responsable del Sistema, quién remitirá la nueva versión actualizada a la dirección o el departamento de Cumplimiento Normativo de la entidad matriz GSSecurity, para su análisis y evaluación.

La citada Comisión evaluará si el contenido del misma continúa siendo adecuado, y lo someterá a la aprobación del Consejo de Administración de la entidad matriz. La evolución que contempla el presente apartado se muestra al comienzo del documentoen 'Control de Versiones' recogiendo cada nueva versión realizada con la fecha de actualización y resumen de las modificaciones realizadas.

El presente Procedimiento entrará en vigor al día siguiente de su aprobación por el Consejo de Administración de la entidad matriz GSSecurity.

GSS SECURITY
Global Security Solutions, S.L.
C.I.F.: B-87093209
C/ Esteban Terradas, 6 - Bajo 2
28914 LEGANÉS (Madrid)

GLOBAL SYSTEM SECURITY
B-64446263 - D.G.P. 4012
C/ Balançó i Boter, 22 2º, 3ª
08302 MATARÓ

Fdo: Iván Roig Almonacid-Nelson Eduardo Menéndez Fernández