Política de uso del *Buzón del Código de Conducta*

Contenido

1. Finalidad

La presente *Política de uso del Buzón del Código de Conducta*, aprobada por el Consejo de Administración, tiene como objeto especificar los criterios de uso de los diferentes canales de comunicación existentes en *EXOLUM* a través de los cuales los *Miembros de la Organización*, *Socios de negocio* y *Terceros pueden enviar Consultas* y/o *Denuncias* sobre posibles *Incumplimientos* que puedan surgir en el seno de la *Organización* en el quehacer de sus actividades.

La *Política de Compliance* penal de *EXOLUM*, detalla los diferentes canales que se pueden emplear a tales efectos.

Todos los *Miembros de la Organización* tienen la obligación de informar sobre comportamientos individuales, colectivos o actividades que concurran en el contexto de sus actividades en *EXOLUM* y que puedan suponer una contravención del contenido del presente texto o del resto de documentos que conforman el *Sistema de gestión de Compliance penal*, con independencia de si tales comportamientos han sido ordenados o solicitados por un superior.

En el **Anexo I** de la presente *Política* se recogen los términos definidos del presente documento.

2. Ámbito de aplicación

2.1. Ámbito de aplicación

La presente *Política* se aplica a todos los Miembros de la Organización, incluyendo aquellas entidades participadas sobre las que se tiene un control efectivo o la responsabilidad de su operación y/o gestión, dentro de los límites previstos en la normativa aplicable. Asimismo, EXOLUM promoverá principios y directrices coherentes con los principios y garantías descritos en esta *Política*, en todas aquellas sociedades y entidades participadas sobre las que no tenga un control efectivo.

Los *Miembros de la Organización* deberán cumplir con su contenido, independientemente de la posición y de la función que desempeñan.

En este sentido, esta *Política* vincula a cualquier persona que pretenda comunicar un posible *Incumplimiento* en un contexto profesional con EXOLUM. Asimismo, vincula a las personas que, aun no siendo empleados, tengan conocimiento de la existencia de cualquier *Incumplimiento* en su relación profesional con EXOLUM como *Socios de negocio* o *Terceros*.

2.2. Actividades afectadas

El alcance de la presente Política abarca a todas las *Consultas* y *Denuncias* que puedan ser planteadas por cualquier *Miembro de la Organización*, *Socios de negocio* y *Terceros*. Las *Comunicaciones* recibidas podrán versar sobre cualquier *Incumplimiento* de la normativa legal que el Informante crea que puede ser aplicable a EXOLUM, así como de cualquier documento que integre el *Sistema de gestión de Compliance penal*.

3. Canales de comunicación

A los efectos de que la presente *Política* tenga una aplicación efectiva, *EXOLUM* pone a disposición de los *Miembros de la Organización*, *Socios de negocio* y *Terceros* diferentes canales internos para que puedan cursar cualquier tipo *Comunicación* que guarde relación con posibles *Incumplimientos*.

En particular, EXOLUM cuenta con las siguientes vías para la consulta o denuncia de prácticas contrarias a los valores o normativa interna de EXOLUM:

a) Comunicaciones escritas:

- Por medio del siguiente enlace en la página web: https://EXOLUM.com/sostenibilidad/transparencia-etica-e-integridad/buzon-del-codigo-de-conducta/
- Por medio del portal corporativo.
- Por medio de la siguiente dirección postal:

  Compliance and Data Protection Lead
  C. Titán, 13
  28045 Madrid (España)

b) Comunicaciones verbales:

- A través de reunión presencial con el *Compliance and Data Protection Lead*.

Los *Miembros de la Organización*, *Socios de Negocio* y *Terceros* podrán solicitar una reunión presencial para la presentación de la *Denuncia*, la cual deberá celebrarse en el plazo máximo de siete (7) días para poder realizar alguna de las *Comunicaciones previstas* en la presente *Política*.

En cualquier caso, en las comunicaciones verbales se advertirá previamente al *Informante* de la grabación de la comunicación o la trascripción de esta y se le informará del tratamiento de sus datos de acuerdo con lo establecido en materia de protección de datos personales.

Independientemente del medio de comunicación utilizado, el *Informante* podrá designar un medio de comunicación preferente para recibir información sobre el estado de su *Denuncia* o puesta en contacto con el mismo para solicitar información y/o aclaración adicional.

EXOLUM anima a todas las personas que sospechen o conozcan de *Incumplimientos* relacionados con *EXOLUM* a que utilicen estos canales internos para hacer llegar a la *Organización* sus *Comunicaciones*.

Toda *Consulta* o *Denuncia* se gestionará por el *Compliance and Data Protection Lead* en los términos descritos en esta *Política* y desarrollados en el *Procedimiento de gestión de informaciones recibidas a través del Buzón del Código de Conducta*.

Además, *EXOLUM* comunica a cualquier posible *Informante* que también podrá informar a las autoridades competentes y si fuera el caso a las instituciones, órganos u organismos de la Unión Europea. A modo enunciativo, el *Informante* podrá acudir a la AII (Autoridad Independiente del Informante), AEPD (Agencia Española de Protección de Datos) www.aepd.es, la CNMC (Comisión Nacional de los Mercados y la Competencia) **www.cnmc.es**, en función de la naturaleza de la irregularidad.

4. Principios y garantías

En lo relativo a dichas *Comunicaciones* de los *Miembros de la Organización*, *Socios de Negocio y Terceros*, *EXOLUM* garantiza la **ausencia de *Represalias y Conductas Perjudiciales***, discriminaciones o sanciones por aquellas *Comunicaciones* realizadas de buena fe o por aquellas actuaciones tendentes a evitar participar en actuaciones delictivas.

En todo caso, la gestión de los canales de comunicación descritos en el apartado anterior está guiada en todo momento por los siguientes principios:

- **Principio de confidencialidad:** se garantizará la confidencialidad de la identidad del *Denunciante* y del *Denunciado*, así como de cualquier otra *Parte Interesada* por la *Denuncia*.

  En este sentido, toda persona que participe en las investigaciones debe mantener la confidencialidad de la información recibida o conocida. Y no puede, por tanto, divulgar a terceros la información conocida en el ejercicio de sus funciones, en especial la relativa a los datos personales.

  La excepción al párrafo anterior tiene que ver con la necesidad de compartir información con las personas involucradas en el caso respetando el *principio de necesidad de conocer* en aquellos casos en que sea estrictamente necesario.

- **Principio de objetividad:** se deben investigar, no sólo los hechos y circunstancias que establecen y agravan la responsabilidad del sujeto de la *Denuncia*, sino también los que le eximan de ella o la extingan o atenúen.

- **Principio de imparcialidad:** la gestión de las denuncias y eventuales investigaciones posteriores se realizarán nombrando a aquellas personas que no tengan ninguna relación con las actividades o negocios afectados. Y, al tiempo, que no tengan ninguna relación con las personas afectadas, al margen de la estrictamente profesional.

- **Principio de confianza:** *EXOLUM* gestionará cualquier *Incumplimiento* comunicado de manera adecuada, seria y objetiva. Asimismo, las gestionará de manera eficaz y transparente, evitando, en todo caso, conculcar el principio de imparcialidad, así como la independencia y autonomía.

- **Prohibición de *Represalias* y demás *Conductas Perjudiciales*:** *EXOLUM* no tolerará ninguna *Represalia* o *Conducta Perjudicial* -por acción u omisión con independencia de que se genere en el ámbito laboral o en el personal- contra quien, de buena fe, comunique hechos que pudieran constituir un *Incumplimiento* conforme a lo dispuesto por esta *Política*, garantizando, para ello, la protección y apoyo necesario desde el momento de interposición de la *Denuncia* hasta el plazo de dos años desde la finalización de la investigación.

- **Principio de proporcionalidad:** este principio responde a la necesidad de que la sanción se ajuste a la gravedad de los hechos, evitando que ésta sea una medida desproporcionada, nutriéndose también de los siguientes principios:

  – Principio de adecuación: las sanciones deben ser las adecuadas al fin que justifican.

  – Principio de suficiencia: las sanciones deben ser suficientes para el fin que persiguen.

  – Principio del "debido proceso": toda persona tiene derecho a ser oído y a hacer valer sus pretensiones legítimas frente a los encargados de la investigación.

– Presunción de inocencia: es el derecho de todo sujeto de la *Denuncia*, a ser tratado como si fuese inocente, hasta que, en su caso, proceda la imposición de una sanción.

5. Derechos del *Informante* y del *Denunciado*

5.1. Derechos del Informante

Los derechos del *Informante* son los siguientes:

- **Derecho a la confidencialidad:** no se revelará la identidad del *Informante* sin su consentimiento expreso a ninguna persona que no sea un miembro autorizado en los términos descritos en esta *Política*. Esto aplica igualmente a cualquier información que pueda permitir que se deduzca la identidad del *Informante*. No obstante, debe tenerse en cuenta que la identidad del Informante puede revelarse cuando esto constituya una obligación en el contexto de un proceso judicial. En este último caso no se requiere el consentimiento del *Informante* para revelar sus datos, sino únicamente un preaviso.
- **Derecho de indemnidad:** se debe garantizar la ausencia de cualquier forma de *Represalia* o *Conducta Perjudicial* contra el Informante por el hecho de haber presentado una *Denuncia*, siempre que sea una *Denuncia de buena fe*, incluidas tanto las amenazas como las tentativas. A estos efectos, se consideran *Represalias* aquellas establecidas en la legislación vigente. Estas garantías de protección al *Informante* se extienden igualmente a terceras personas involucradas en el proceso de *Denuncia* que pudieran sufrir consecuencias negativas por ello (entre otros, testigos, compañeros de trabajo o familiares del *Informante* o personas jurídicas para las que trabaja o mantiene una relación en un contexto laboral el *Informante*).

5.2. Derechos del Denunciado

Los derechos del *Denunciado* son los siguientes:

- **Derecho a evitar daños a la reputación del Denunciado:** los derechos de la persona afectada deben estar protegidos para evitar daños a la reputación u a otras consecuencias negativas, preservando su derecho de presunción de inocencia durante todo el proceso de investigación.
- **Derecho a la confidencialidad** de la identidad del *Denunciado* y que su identidad esté protegida durante todo el procedimiento.
- **Derecho de defensa:** se deben garantizar los derechos de defensa del *Denunciado*, incluido el derecho de acceso al expediente, el derecho de conocer el estado del procedimiento, el derecho a ser oído y el derecho a una tutela judicial efectiva contra una decisión que le concierna en el contexto de investigaciones o procesos judiciales ulteriores.
- **Derecho a la información, trámite de audiencia y acceso al expediente:** se debe garantizar al *Denunciado* el conocimiento oportuno de las acciones u omisiones que se le atribuyen y a ser oído en cualquier momento desde el conocimiento de los hechos con los que se le relacionan.
- **Derecho a la presunción de inocencia y al honor como sujeto afectado:** todo *Denunciado* deberá ser tratado como si fuese inocente, hasta que, en su caso, proceda la imposición de una sanción.

En cuanto al derecho de acceso al expediente, cabe destacar que su ejercicio debe respetar el derecho de confidencialidad del *Informante*, así como del resto de personas que han intervenido en el procedimiento de investigación, por ejemplo, en calidad de testigos. Por ello, deberá garantizarse que el *Denunciado* no accede a los documentos, grabaciones u otros soportes en los que se identifique a persona físicas intervinientes en el proceso de investigación y/o a manifestaciones o relatos de hechos que éstas hayan realizado. Deberá garantizarse el acceso por parte del *Denunciado* a un resumen de los hechos investigados, a las diligencias practicadas (con las limitaciones antes indicadas), y a la resolución, incluyendo los motivos que la justifican.

Así mismo, en caso de no encontrarse evidencias de *Irregularidades* y que la *Denuncia* haya sido impuesta de mala fe, el *Denunciado* tiene la posibilidad de solicitar a la *Organización* considerar la posibilidad de imponer medidas correctivas para el *Informante*.

5.3. Medidas de apoyo

La protección implicará la adopción de medidas razonables para evitar que se produzcan daños y que se ponga en peligro la confidencialidad del *Informante*, *Denunciado* o *Terceros*.

Por su parte, el apoyo implicará alentar y tranquilizar al *Informante* o a los *Terceros* sobre el valor de informar de *Incumplimientos* y tomar medidas para ayudar a su bienestar.

Por otro lado, el apoyo será también dirigido a los *Denunciados* en cuanto a la confidencialidad de su identidad, garantía del derecho de defensa y de acceso al expediente para tener conocimiento de las acciones u omisiones que se le atribuyen.

La protección y el apoyo brindados al *Informante*, los *Terceros* implicados y los *Denunciados* activarán y darán comienzo tan pronto como se reciba una *Consulta* o una *Denuncia*, y continuará durante y después de la conclusión del proceso de investigación, e incluso después durante un período máximo de dos años desde que finalice la investigación del *Incumplimiento*.

Una vez transcurrido el plazo de dos años, se podrá solicitar una prórroga a la *Autoridad Independiente de Protección del Informante* que, excepcionalmente y de forma justificada, podrá extender el período de protección, previa audiencia de las personas u órganos que pudieran verse afectados.

El *Compliance and Data Protection Lead* será responsable de asegurar que dichas medidas de apoyo y protección se implementen en *EXOLUM*.

6. Roles y responsabilidades

El *Consejo de Administración* ha designado al *Compliance and Data Protection Lead* como *Responsable del Sistema interno de Información* conforme a lo dispuesto en la presente Política.

6.1. Responsabilidades del *Compliance and Data Protection Lead* como *Responsable del Sistema interno de Información*

Los roles y responsabilidades del *Responsable del Sistema interno del Información* en relación con las *Consultas* y *Denuncias* recibidas son los siguientes:

- Recepción de todas las *Consultas* y *Denuncias* recibidas mediante los canales de comunicación detallados en el apartado 3 de la presente *Política*.
- Guardar registro de la trazabilidad documental de las *Denuncias* en el *Libro-registro de informaciones*, así como del resto de evidencias documentales.
- Análisis de las comunicaciones remitidas con rigor, independencia, autonomía, objetividad y confidencialidad.
- Comunicar al *Consejo de Administración*, a través del *Comité de Auditoría*, y/o al *Comité de Dirección*, los *Incumplimientos* de la normativa aplicable a *EXOLUM* de los que tenga conocimiento que puedan generar responsabilidad penal para la *Organización*.
- Ejecutar el *Procedimiento de gestión de informaciones recibidas a través del Buzón del Código de Conducta*, desde la recepción de la *Denuncia* hasta su resolución.
- Mantener un contacto constante y fluido con el *Informante* durante la tramitación de su *Denuncia o Consulta*.
- Emisión del informe sobre la *Denuncia*.

7. Denuncias de mala fe

La protección y apoyos brindados por *EXOLUM* estarán sujetos a que el *Informante* haya interpuesto la *Denuncia* actuando de buena fe.

El *Informante* debe tener motivos razonables para creer, a la luz de las circunstancias y de la información de que disponga, que los hechos que denuncia son ciertos. En este sentido, la buena fe supone denunciar teniendo, al menos, motivos razonables para creer que la información sobre posibles infracciones comunicada era cierta en el momento de informar.

Además, *EXOLUM* analizará cada caso concreto a los efectos de imponer medidas disciplinarias proporcionadas frente a los *Miembros de la Organización* o mercantiles frente a *Socios de negocio y Terceros* que interpongan una *Comunicación* de mala fe.

8. Protección de datos personales

EXOLUM tratará los datos recibidos a través del *Buzón del Código de Conducta* y los otros canales de comunicación de conformidad con la normativa vigente en materia de protección de datos. El tratamiento de los datos personales será con la finalidad de gestionar y resolver cualquier *Consulta* o *Denuncia*, así como para analizar la criticidad de los hechos comunicados, realizar en su caso una investigación sobre los posibles *Incumplimientos*, adoptar las medidas cautelares necesarias y en el caso de que sea necesario, iniciar las acciones internas o legales que correspondan.

Para poder cumplir con dichas finalidades se deberán recabar determinados datos personales e información, ya sea directamente a través del *Informante*, a través de la/s persona/es que determine la *Organización* o a través de *Terceros* autorizados contratados específicamente a tales efectos, que garantizarán el más alto nivel de confidencialidad y seguridad técnica.

Todos los *Miembros de la Organización* están obligados y especialmente en el ámbito del *Buzón del Código de Conducta*, a facilitar información propia, cierta, veraz y lícita, siendo los únicos responsables de las manifestaciones falsas o inexactas que proporcionen, así como de las consecuencias internas, administrativas y/o legales que sean de aplicación.

La *Organización* velará en todo caso porque los distintos canales de comunicación constituyan un medio seguro, dotado de las medidas requeridas por la normativa sobre Protección de Datos Personales y seguridad de la información.

8.1. Conservación de la información

EXOLUM tratará, gestionará y conservará la información y los datos personales contenidos en las *Denuncias*, investigaciones, informes y demás documentación de acuerdo con los plazos establecidos en la normativa vigente en materia de protección de datos y demás normativa de aplicación. Dicha información, además, estará custodiada por el *Compliance and Data Protection Lead* y será suprimida, bloqueada o anonimizada finalizados los plazos legales y de acuerdo con lo especificado en la Política de Tratamiento de Datos de Carácter Personal de Exolum.

9. Monitorización y revisión de la Política

El *Compliance and Data Protection Lead* es el principal responsable de la supervisión y aplicación de esta *Política*, así como de que la misma sea revisada periódicamente.

La monitorización de la presente *Política* incluye (i) las revisiones periódicas de la efectividad de la formación de los empleados en lo que concierne a estas cuestiones, (ii) reportes y registros de las incidencias relacionadas con la presente *Política*, y la revisión de su adecuación a la legislación vigente.

ANEXO

Definiciones

Se relacionan a continuación las definiciones de aquellos conceptos (citados en *cursiva*) que se utilizarán de manera frecuente en el presente documento y en las normas relacionadas que conforman el *Sistema de gestión de Compliance penal de GRUPO EXOLUM*.

- ***GRUPO EXOLUM / la Organización:*** formado por la sociedad EXOLUM CORPORATION S.A. como matriz del grupo, así como por el resto de las entidades que forman parte del *Perímetro de control penal*.
- ***Perímetro de control penal:*** incluye a las entidades adheridas al *Sistema de gestión de Compliance penal* de *GRUPO EXOLUM*, relacionadas en el Anexo I de la Política de *Compliance* penal.
- ***Consejo de Administración:*** máximo órgano de decisión de EXOLUM CORPORATION, S.A., como sociedad matriz de *GRUPO EXOLUM*, con competencias de decisión en materias relacionadas con la gestión corporativa de la *Organización* a nivel global.
- ***Comité de Auditoría:*** Comité responsable del cumplimiento del Código de Conducta, las políticas que lo desarrollan y la eficiencia de los controles internos establecido para mitigar el riesgo de incumplimiento.
- ***Comité de Dirección (Executive Committee):*** órgano interno de dirección y control para el normal funcionamiento de EXOLUM CORPORATION, S.A., que informa periódicamente al Consejo de Administración de las circunstancias más importantes de la gestión de la Compañía y su Grupo.
- ***Compliance and Data Protection Lead:*** órgano unipersonal responsable de supervisar el funcionamiento y observancia del *Sistema de gestión de Compliance penal* de la *Organización*, dotado de poderes autónomos de iniciativa y control. La existencia del *Compliance and Data Protection Lead* responde a las exigencias establecidas en la normativa española (artículo 31 bis del Código penal español) en cuanto a la supervisión del *Sistema de gestión de Compliance penal*.
- ***Sistema de gestión de Compliance penal:*** sistema de organización y gestión para la prevención de delitos, cuyo objetivo es la prevención, detección y gestión de *Riesgos penales*, y cuya base esencial se representa en la *Política de Compliance penal*.
- ***Miembros de GRUPO EXOLUM / Miembros de la Organización:*** integrantes del *Consejo de Administración*, miembros del *Comité de Dirección*, empleados, trabajadores temporales o bajo convenio de colaboración y el resto de las personas bajo subordinación jerárquica de cualquiera de los anteriores.
- ***Socios de negocio:*** cualquier persona jurídica o física, salvo los *Miembros de la Organización*, con quien la *Organización* mantiene o prevé establecer algún tipo de relación de negocios. A modo enunciativo, pero no limitativo, se incluyen proveedores, asesores externos, clientes y, en general, personas físicas o jurídicas contratadas por *GRUPO EXOLUM* para el desarrollo de su actividad.
- ***Tercero:*** persona física o jurídica u órgano que es independiente de la *Organización*.
- ***Sistema Interno de Información:*** medidas adoptadas conforme 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 (o también referida Ley de Protección al Informante) para la gestión de comunicaciones relativas a infracciones de la normativa a que se refiere dicho texto.
- ***Responsable del Sistema interno de Información:*** *Grupo EXOLUM* ha designado como *Responsable del Sistema Interno de Información* al *Compliance and Data Protection Lead*, teniendo el mismo carácter directivo, siéndole encomendadas las funciones propias de gestión del *Sistema Interno de Información* y de tramitación de expedientes de investigación en calidad de notificar su designación a la *Autoridad Independiente de Protección al Informante (A.A.I)*.
- ***Comunicación:*** declaración por la que cualquier *Miembro de la Organización o Tercero* deja constancia de una cuestión acerca del alcance, interpretación o cumplimiento de la Normativa aplicable a la *Organización*. En función de su contenido, una *Comunicación* puede contener una *Consulta* o una *Denuncia*.

- ***Consulta:*** comunicación por la que cualquier *Miembro de la Organización* o *Tercero solicita* una aclaración, respuesta o criterio sobre el alcance, interpretación o cumplimiento de la normativa aplicable a *GRUPO EXOLUM*.
- ***Denuncia:*** comunicación relativa a un posible *Incumplimiento* de la normativa aplicable a GRUPO *EXOLUM*.
- ***Informante:*** persona física o jurídica que interpone una *Consulta* o *Denuncia*. La figura del Informante incluye a los *Miembros de la Organización*, *Socios de negocio*, *Terceros* y cualquier persona, con un encaje presente o futuro, en los contextos anteriores.
- ***Denunciado:*** persona física o jurídica a la que se le imputa un presunto *incumplimiento* objeto de investigación por parte del *Compliance and Data Protection Lead* de *GRUPO EXOLUM*.
- ***Incumplimiento:*** comportamiento, activo u omisivo que suponga la infracción de la Normativa aplicable a *GRUPO EXOLUM*. Un *Incumplimiento*, en función de su gravedad, puede abarcar desde el mero *Incumplimiento* formal de un requisito incluido en una norma interna, hasta la comisión de hechos constitutivos de un delito potencialmente imputable a GRUPO EXOLUM.
- ***Notificación:*** acción de informar a las partes involucradas en el procedimiento, a fin de garantizar el correcto desarrollo del mismo y el respeto a sus derechos.
- ***Denuncia de buena fe:*** *denuncia* que se realiza conforme a lo dispuesto en la presente *Política* y está basada en hechos o indicios de los que razonablemente pueda desprenderse la existencia de un *Incumplimiento* de la legislación vigente o de la normativa interna. Se considera que la *Denuncia* es de buena fe cuando la misma se realiza sin ánimo de venganza o de causar un perjuicio laboral o profesional al *Denunciado* o a un *Tercero*.
- ***Libro-registro de las informaciones:*** herramienta utilizada por el *Responsable del Sistema interno de Información* para asegurar la trazabilidad y seguridad de las comunicaciones recibidas por el canal dispuesto por *GRUPO EXOLUM* a tal efecto.
- ***Autoridad Independiente de Protección del Informante (AAI):*** autoridad administrativa independiente, como ente de derecho público de ámbito estatal, que actuará en el cumplimiento de su función principal de protección a los *Informantes*. Entre sus otras funciones a destacar, se encuentra la gestión de su propio canal externo, la tramitación de procedimientos sancionadores y, la imposición de sanciones, entre otras.
- ***Represalias y Conductas Perjudiciales:*** cualquier acción u omisión, ya sea tentativa, amenaza o materializada, directa o indirectamente, de la que se pueda desprender un daño o desventaja, para el Informante, en el ámbito laboral o profesional, solo por su condición en relación con la Denuncia o por haber realizado una revelación pública.
- ***Procedimiento de gestión de informaciones recibidas a través del Buzón del Código de Conducta:*** documento que establece los mecanismos necesarios para la comunicación y gestión de manera temprana de cualquier *Incumplimiento*, así como los procedimientos necesarios para la tramitación interna de *Consultas*, y tramitación e instrucción interna de aquellas *Denuncias* o cualquier circunstancia conocida que deba ser investigada.

Titán, 13. 28045 Madrid (España)
Tel.: +34 91 774 60 00
www.exolum.com