POLÍTICA DE GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN (Canal de denuncias)

Nº Inscripción CNMV: 244

AAA.114503
05/10/2026

ÍNDICE

1. INTRODUCCIÓN 3
1.1 Antecedentes 3
1.2 Ámbito de aplicación 3
1.3 Ámbito subjetivo 3
1.3.1 ¿Qué se entiende por informante? 3
1.3.2 ¿Sobre quién se puede informar? 4
1.4 Ámbito objetivo 4
2. PRINCIPIOS GENERALES DEL SISTEMA INTERNO DE INFORMACIÓN 4
3. DERECHOS Y DEBERES DEL INFORMANTE 5
3.1 Derechos 5
3.2 Deberes 6
4. DERECHOS DEL AFECTADO 6
5. IDENTIFICACIÓN DE CANALES 6
5.1 Canal de denuncias 6
5.2 Canal Externo de Información 7
6. PROCEDIMIENTO 7
7. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL 11
8. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN 12
9. PUBLICIDAD Y DIVULGACIÓN 12
10. REVISIÓN Y ACTUALIZACIÓN 13

1. INTRODUCCIÓN

1.1 Antecedentes

Con la aprobación de 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 se traspone al Derecho español la Directiva (UE) 2019/1937 del Parlamento y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.

En cumplimiento con lo establecido en la Ley 2/2023, COVENTINA PARTNERS EAF, S.L. (en adelante, Coventina) aprueba la presente Política de Gestión del Canal Ético. El objetivo de esta Política es establecer las garantías para la protección de los informantes, los principios generales que regulan el funcionamiento del Sistema Interno de Información y el procedimiento de gestión de informaciones cuya finalidad es establecer las previsiones necesarias para que el Sistema Interno de Información cumpla con los requisitos establecidos en la Ley 2/2023.

1.2 Ámbito de aplicación

La presente Política es aplicable a todos los departamentos y áreas Coventina. En consecuencia, deberán tomarse las decisiones necesarias para integrar las disposiciones de esta Política, siguiendo el principio de proporcionalidad, y ajustándose al marco de gobierno, principios de actuación, metodologías y procesos descritos en este documento. El incumplimiento de esta Política podrá dar lugar al ejercicio de medidas disciplinarias por parte del órgano interno competente. En el caso de relaciones mercantiles con terceros, podría derivar en la terminación de los contratos vigentes.

1.3 Ámbito subjetivo

1.3.1 ¿Qué se entiende por informante?

Los informantes pueden reportar o comunicar sobre acciones u omisiones incluidas en el ámbito de esta Política a través de los distintos Canales que forman parte del Sistema Interno de Información. A efectos de esta Política, se considera como informante a:

- Empleados, directivos y Administradores de Coventina.
- Becarios.
- Trabajadores de empresas de trabajo temporal.
- Accionistas.
- Colaboradores.
- Proveedores y personas bajo su supervisión.
- Clientes o potenciales clientes.
- Exempleados.
- Candidatos a un puesto de trabajo.
- Terceras partes con las que exista algún tipo de relación o vínculo.
- Cualquier persona que haya detectado una conducta ilícita.

1.3.2 ¿Sobre quién se puede informar?

Se podrán reportar acciones o informar sobre empleados, directivos, Administradores, o colaboradores externos de Coventina que estén bajo su autoridad y que hayan incurrido en alguna irregularidad o conducta recogida dentro del ámbito objetivo especificado en esta Política.

1.4 Ámbito objetivo

A través de los diversos Canales que forman parte del Sistema Interno de Información, los informantes pueden reportar cualquier conocimiento o sospecha fundamentada sobre conductas irregulares, que se detallan en el Anexo y se enumeran a continuación:

1. Incumplimientos o infracciones de los principios establecidos en el Código Ético.

2. Actos o conductas que puedan tener relevancia penal.

3. Cualquier acción u omisión que pueda constituir una infracción del Derecho de la Unión Europea.

4. Cualquier otra irregularidad que pueda generar responsabilidad para Coventina.

2. PRINCIPIOS GENERALES DEL SISTEMA INTERNO DE INFORMACIÓN

El Sistema Interno de Información se rige por los siguientes principios generales:

Protección del informante

Este es el principio fundamental de la Política, garantizando un régimen específico que protege a quienes informen sobre infracciones normativas frente a posibles represalias.

Protección de las personas afectadas

El Sistema brindará a las personas involucradas en la comunicación la misma protección que se otorga a los informantes.

Confidencialidad

Se asegurará la máxima confidencialidad sobre la identidad del informante, las personas mencionadas, la información proporcionada y las acciones derivadas del proceso.

Anonimato

El Sistema permitirá que las denuncias se realicen de manera anónima, implementando las medidas técnicas y organizativas necesarias para proteger el anonimato cuando el informante así lo decida.

Independencia y autonomía

El Responsable del Sistema ejercerá sus funciones de forma independiente y autónoma respecto a los demás órganos de la entidad, garantizando un tratamiento imparcial y justo hacia las personas involucradas.

Transparencia y accesibilidad

Se garantizará que la información sobre el Sistema y su regulación sea clara, comprensible y accesible para todos.

Diligencia

Se asegura que la investigación y resolución de los hechos denunciados se realicen con profesionalidad, diligencia y sin retrasos injustificados.

Buena fe

A pesar de posibles inexactitudes o errores no intencionados por parte del informante, se buscará que la información proporcionada sea honesta, íntegra y veraz.

3. DERECHOS Y DEBERES DEL INFORMANTE

3.1 Derechos

Las personas que informen sobre infracciones contempladas en esta Política tienen derecho a protección contra represalias, siempre que existan motivos razonables para creer en la veracidad de la información y que la comunicación haya sido realizada de buena fe y conforme a los requisitos establecidos en esta Política.

Coventina prohíbe expresamente cualquier acto de represalia contra quienes presenten una comunicación conforme a lo dispuesto en esta Política.

Se entiende por represalia cualesquiera actos u omisiones prohibidos por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, solo por su condición de informantes.

Cualquier forma de represalia contra un informante que haya actuado de buena fe será sancionada. En caso de que el informante perciba o tema represalias como consecuencia de su comunicación, podrá informar al Responsable del Sistema Interno para que se tomen las medidas adecuadas para prevenir o corregir dichas represalias.

No obstante lo anterior, quedarán excluidos de la protección prevista en la presente Política:

- Quienes comuniquen o revelen información contenida en comunicaciones que hayan sido inadmitidas.
- Quienes comuniquen cuestiones relacionadas con conflictos interpersonales o que afecten únicamente al informante y a las personas implicadas.
- Quienes comuniquen información que ya sea de dominio público o que se base en meros rumores.
- Quienes informen sobre hechos o situaciones fuera del ámbito de aplicación de esta Política.

El informante también tendrá derecho a conocer el estado de la tramitación de su comunicación y los resultados de la investigación y ejercer los derechos que le confiere la legislación de protección de datos de carácter personal.

Coventina deberá garantizar que el informante pueda decidir si desea formular la comunicación de forma anónima o no anónima y, en este segundo caso, se garantizará la máxima confidencialidad acerca de la identidad del informante.

3.2 Deberes

El informante tiene como deber actuar de buena fe y denunciar como mínimo por sospechas razonadas. En caso contrario, podrán establecerse las medidas disciplinarias o sancionadoras que procedan cuando la investigación interna determine que la denuncia es falsa y que la persona la ha realizado consciente de su falsedad y actuando de mala fe.

El informante también tiene el deber de aportar los datos y documentos de que disponga que guarden relación con los hechos denunciados, y de mantener, en la medida de lo posible, la máxima confidencialidad durante la tramitación de la denuncia y el desarrollo de la investigación interna que pudiera derivarse.

4. DERECHOS DEL AFECTADO

Las personas afectadas por la comunicación tendrán derecho a la presunción de inocencia, al derecho de defensa y al derecho de acceso al expediente, con excepción de la identidad del informante y de las otras personas afectadas, durante la tramitación del expediente y de la investigación interna. Asimismo, dispondrá de la misma protección establecida para los informantes, debiéndose preservar su identidad y garantizar la confidencialidad de los hechos y datos del procedimiento.

La identidad del informante sólo podrá ser comunicada a la Autoridad Judicial, al Ministerio Fiscal o a la Autoridad Administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.

La persona afectada será informada de la existencia de la comunicación, de los hechos de los que se le atribuyen, y de la posibilidad de ejercer los derechos que le correspondan. No obstante, cuando exista un riesgo importante de que dicha notificación pudiera poner en peligro la capacidad de Coventina para investigar de manera eficaz los hechos, la notificación podrá demorarse mientras exista dicho riesgo.

Asimismo, el afectado tendrá derecho a que se le informe de la correspondiente resolución.

5. IDENTIFICACIÓN DE CANALES

5.1 Canal de denuncias

El Canal Ético de Coventina es la vía principal para informar sobre posibles irregularidades que puedan suponer infracciones que versen sobre actos o conductas, presentes o pasadas, referidas a los ámbitos de aplicación detallados en el Anexo. Así como la realización de consultas sobre cómo actuar de acuerdo a la ley o la normativa interna de la Sociedad.

- Este Canal permite la presentación de comunicaciones por escrito a través de la Plataforma corporativa accesible a través del siguiente enlace: https://canal-etico.lant-abogados.com/Specific/MVistaPublica?codiClient=MDA0OTg1&secure=464243.0

- A solicitud por escrito del informante, también se podrá presentar una denuncia, mediante una reunión presencial dentro del plazo de siete días desde la recepción de la solicitud.

5.2 Canal Externo de Información

Sin perjuicio del acceso al canal interno detallado (canal ético) y en cualquier momento, toda persona física que forme parte de algunos de los colectivos con acceso al Sistema Interno de Información puede dirigirse a la Autoridad Independiente de Protección del Informante (A.A.I.) o ante las autoridades u órganos autonómicos correspondientes, para informar de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación de la Ley 2/2023.

6. PROCEDIMIENTO

Como se mencionó previamente, el Sistema Interno de Información está respaldado por una serie de principios y garantías que han dado forma al siguiente procedimiento. En este, se pueden distinguir las siguientes fases:

6.1 Fase de registro

Toda persona con acceso al Sistema Interno de Información podrá dirigir la comunicación al Canal de Denuncias, en cumplimiento del principio de la buena fe.

Una vez el informante acceda a la plataforma tendrá que clicar en "Crear una denuncia". Una vez en la página de Nueva denuncia, podrá elegir si quiere facilitar o no sus datos personales (nombre y apellidos, email, teléfono). Si desea permanecer en el anonimato no deberá cumplimentar ninguno de esos campos.

A continuación, deberá seleccionar cuál es su relación con la empresa entre las que se indican en el menú desplegable (cliente, empleado, proveedor, otro).

Una vez lo indique, deberá describir con sus propias palabras lo sucedido en el apartado "Texto denuncia".

El informante también podrá adjuntar archivos que documenten y acrediten su comunicación. No obstante, el informante podrá ampliar la información y documentación de la comunicación con posterioridad a su formulación, ya sea de manera voluntaria o por solicitud del Responsable del Sistema. Los nuevos hechos y documentación aportada serán considerados en el proceso de gestión.

Una vez haya cumplimentado todos los campos, deberá pulsar en enviar.

Finalmente, aparecerá una pantalla confirmando que su caso ha sido enviado y se le pedirá que guarde su código de seguimiento, ya que necesitará el mismo para iniciar sesión y consultar el estado de su denuncia.

En el caso de comunicaciones presentadas por otras vías distintas de la plataforma del Canal de Denuncias ya se trate de comunicaciones realizadas por el propio informante como aquellas remitidas al Responsable del Sistema por parte del canal o del receptor no

responsable de la gestión, serán incorporadas al Canal de Denuncias corporativo una vez obtenida la información.

6.2 Fase de análisis

Una vez recibida la comunicación, se emitirá acuse de recibo al informante en el plazo máximo de siete (7) días naturales. A continuación, se procederá a realizar el análisis de la denuncia con el objeto de determinar si es admitida para su tramitación y gestión.
Serán causa de inadmisión de la denuncia, entre otras, las siguientes:

a) Cuando el contenido de la denuncia se refiera a conductas, hechos o informaciones que no se encuentren incluidos dentro del ámbito de aplicación de esta Política.

b) Cuando el contenido de la denuncia recoja informaciones ya disponibles al público en general, o se trate de meros rumores.

c) Por falta de verosimilitud cuando los hechos sean manifiestamente infundados y sin acreditación alguna.

d) Cuando carezca de información nueva o significativa respecto de otras comunicaciones anteriores.

e) Cuando existan indicios de que la información se ha obtenido ilícitamente.

f) Cuando se trate de informaciones vinculadas a reclamaciones sobre conflictos interpersonales que afecten únicamente al informante y a las personas a las que se refiera la comunicación o revelación.

g) Cuando la descripción de los hechos sea genérica o imprecisa, haciendo imposible la concreción e investigación de las supuestas irregularidades denunciadas. Previo a la inadmisión por esta causa, el responsable del canal comunicará al denunciante, cuando la denuncia no haya sido anónima, las deficiencias de su denuncia a fin de que aclare y precise debidamente los hechos a que se refiera. De no subsanarse tales deficiencias se procederá a la inadmisión.

En todos los casos de inadmisión se trasladará al informante de la decisión motivada, lo que se llevará a cabo a través del buzón de comunicación de la plataforma al que podrá acceder el informante con el código ID de acceso generada a tal efecto por el Canal, siempre que la comunicación haya sido realizada a través del enlace habilitado en la página web, o empleando los datos de contacto que en su caso hubiera facilitado el informante.

No obstante, el Responsable del Sistema se reserva la potestad de admitir una comunicación que, a pesar de no cumplir los criterios de admisibilidad, concurra en ella un supuesto de hecho excepcional que requiera de gestión a través del Sistema Interno de Información.

En el marco de la gestión de la comunicación, ya sea antes y/o después de su admisión, puede resultar necesario contactar con el informante para solicitar información adicional, aclarar algún aspecto o, incluso, realizar un acompañamiento. La plataforma dispone de un sistema de comunicación encriptada que permite la comunicación entre responsable e informante.

En caso de admisión, se iniciarán las diligencias de análisis a practicar, entre las que se encuentran la interacción con las partes interesadas y las comunicaciones y cumplimiento de los requisitos en materia de protección de datos personales. En caso de inadmisión, se finalizará la gestión del expediente y así se comunicará al informante.

Si la comunicación es admitida, se procede a su registro en la plataforma y se continúa con su gestión. Adicionalmente, y en cumplimiento con lo establecido en la Ley 2/2023 se mantiene un libro-registro de las informaciones recibidas, que recogerá todas las gestiones realizadas y las investigaciones internas que hayan dado lugar, garantizando la confidencialidad de la información.

En caso de existir persona afectada se comunica la recepción de la comunicación contra su persona y en paralelo se da traslado al equipo que vaya a realizar la investigación.

Excepcionalmente, en aquellos casos en los que la comunicación realizada al afectado podría poner en peligro el curso de la investigación de los hechos/conductas objeto de comunicación, podrá demorarse la comunicación, pero esta no podrá superar en ningún caso el plazo de 1 mes desde que se haya registrado.

En todo caso, la comunicación incluirá:

- la recepción de la comunicación y la fecha,
- las conductas/hechos que se le atribuyen,
- el equipo responsable de su gestión, y
- el tratamiento que se realizará de sus datos de carácter personal.

La fase de análisis de la comunicación finaliza con la selección del equipo responsable de la investigación, que recaerá en la Unidad de Cumplimiento Normativo, sin perjuicio de que, según la especialidad de los hechos objeto de la comunicación deban intervenir otras áreas siempre que así se requiera para su resolución.

6.3 Fase de investigación

Una vez recibida y admitida a trámite la comunicación, el plazo máximo para la realización de la investigación será de tres (3) meses a contar desde la recepción de la comunicación, salvo casos en que la especial complejidad del asunto requiera una ampliación, en cuyo caso, el plazo podrá extenderse hasta un máximo de otros tres (3) meses adicionales.
La investigación se llevará a cabo de acuerdo con los procedimientos internos definidos, en cumplimiento de las garantías previstas en esta Política. El procedimiento de investigación podrá incluir:

- Entrevistas personales con la fuente (informante) para recabar más información.
- Entrevistas personales con los departamentos y/o las personas involucradas de manera directa o indirecta en los hechos/conductas que potencialmente son irregulares, a criterio del equipo responsable de la investigación.
- Análisis de datos y obtención de información.
- Petición de pruebas periciales a profesionales internos o externos.

- Otras diligencias de investigación o prueba que se consideren pertinentes y sean lo menos gravosas posibles con relación a la posición jurídica de la persona afectada.

El proceso de investigación quedará debidamente documentado, detallando los antecedentes, el objetivo, el alcance y las conclusiones alcanzadas.

Especialmente en el curso de la investigación, pero también con anterioridad a esta, podrá resultar necesario aplicar determinadas medidas de protección, tales como la eliminación de la coincidencia del lugar de trabajo o la gestión de incompatibilidades caso de que alguna de las personas implicadas en una comunicación tuviese relación de parentesco, afinidad o de consanguinidad con alguno de los intervinientes en su gestión, investigación o resolución.

Estas medidas de protección también se aplicarán, en su caso, a:

- Los representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante.
- Personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso.
- Personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante.
- Personas jurídicas, para las que trabaje o con las que mantengan cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa.

6.4 Fase de resolución

Se elaborará un informe y se propondrá la resolución del expediente a partir de las conclusiones obtenidas durante la fase de investigación. Este informe final se comunicará a los informantes, los afectados y a aquellas personas o responsables de Departamentos que deban ejecutar la resolución o conocer de su contenido.

El Responsable del Sistema remitirá el expediente al departamento de Recursos Humanos, para la toma de las medidas oportunas, en caso de identificarse algún incumplimiento por parte de una persona trabajadora. Si la propuesta de resolución contempla la adopción de medidas de otra naturaleza, el expediente se remitirá a la instancia competente que corresponda por razón de la materia o naturaleza de las medidas.

6.5 Conservación de la información

La información se alojará y conservará de acuerdo con los requerimientos legales que en esta materia resulten de aplicación en cada caso. El tratamiento de datos personales será, igualmente, adecuado a las legislaciones aplicables en la materia. Se considerarán, en cualquier caso, los posibles requerimientos de Administraciones públicas, juzgados y tribunales, en los términos establecidos por la legislación en vigor, y únicamente durante el plazo de prescripción de las acciones que se puedan derivar del tratamiento en cuestión.

7. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El Sistema Interno de Información está diseñado, establecido y gestionado de forma segura, de modo que se garantiza la confidencialidad de las personas involucradas en las comunicaciones y de las actuaciones que se desarrollan en la gestión y tramitación de estas, así como de la protección de datos.

Los tratamientos de datos personales que deriven de la aplicación de la Ley 2/2023 se regirán por lo dispuesto en el Título VI de esta y en la legislación aplicable en esta materia.

A los informantes se les informará de que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros. Así mismo, no se informará, en ningún caso, a la persona a la que se refieran los hechos relatados de la identidad del informante.

El acceso a los datos personales contenidos en el Sistema Interno de Información quedará limitado a las personas con potestad de gestión según las funciones que tienen asignadas, quedando expresamente prohibido divulgar cualquier tipo de información sobre las comunicaciones a personas no autorizadas. En cualquier caso, el acceso a estos datos quedará restringido, dentro del ámbito de sus competencias y funciones, exclusivamente a:

- El responsable del Sistema.
- El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.
- Los encargados del tratamiento designados.
- El delegado de protección de datos.

Será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas correctoras en la Entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

No se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una información específica o, si se recopilan por accidente, se eliminarán sin dilación indebida.

Los datos personales que sean objeto de tratamiento se conservarán en el Sistema Interno de Información únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados. Si se procede a la inadmisión de la comunicación por no cumplir con los criterios de admisibilidad definidos, se procederá a la supresión de los datos, salvo que la inadmisión se produjera por la falta de veracidad de la comunicación y ello pudiera constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

En todo caso, transcurridos tres (3) meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, se procederá a la supresión de los datos personales, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del Sistema Interno de Información. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo.

Los colectivos con acceso al Sistema Interno de Información serán informados acerca del tratamiento de datos personales.

No obstante lo anterior, el interesado puede ejercer los derechos de acceso, rectificación, supresión, limitación, oposición y portabilidad mediante correo electrónico en la dirección de correo electrónico dpo@grupolmg.es o en nuestro domicilio postal, en C/Príncipe de Vergara 12, 1º A, 28001 – Madrid, acreditando siempre su identidad, o bien ante la Agencia de Protección de Datos si entiende que no ha obtenido satisfacción en el ejercicio de los derechos indicados.

8. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN

Los Administradores de Coventina serán los responsables de nombrar un responsable del Sistema Interno de Información.

El Responsable del sistema, desarrolla sus funciones de forma independiente y autónoma y debe disponer de todos los medios personales y materiales necesarios para llevarlas a cabo.

Tanto el nombramiento como el cese del responsable del sistema deberá comunicarse en el plazo de 10 días hábiles a la Independiente de Protección del Informante (A.A.I.) o ante las autoridades u órganos autonómicos correspondientes. Para el supuesto del cese, deberán indicarse las causas.

Las personas incluidas en el ámbito de aplicación de la presente Política están obligadas a colaborar con el Responsable del Sistema en los términos de la presente Política.

El responsable interno de información tiene como obligaciones:

- Proporcionar a los Administradores de Coventina, con el tiempo suficiente, información exacta, clara y suficiente que facilite la toma de decisiones y permita verificar que se está operando dentro de la tolerancia al riesgo marcada.
- Satisfacer los requerimientos de información de los organismos supervisores.

Además, el responsable del sistema interno de información:

- Podrá solicitar la información necesaria para garantizar el cumplimiento de las disposiciones legales en las diferentes áreas y/o departamentos de la sociedad.
- Facilitará de forma periódica información relevante sobre el sistema de información interno a los Administradores de Coventina.

9. PUBLICIDAD Y DIVULGACIÓN

Sin perjuicio de la obligación que tienen las personas incluidas en el ámbito de aplicación de la presente política de conocer y actuar de conformidad con lo dispuesto en la Normativa Interna de la sociedad en el desempeño de sus funciones, se promoverá y velará por la debida difusión de esta Política y de la existencia del Canal de Denuncias.

10. REVISIÓN Y ACTUALIZACIÓN

La presente Política se someterá a revisión por parte la Unidad de Cumplimiento Normativo anualmente y en su caso, si se produjera alguna modificación, será aprobada por los Administradores de Coventina.

Adicionalmente, la actualización de la Política se podrá iniciar, en cualquier momento y a petición de cualquiera de los implicados en la gestión del riesgo de conducta y cumplimiento que haya identificado la necesidad de su modificación, por:

- Cambios en el marco normativo.
- Cambios en los objetivos y estrategia de negocio.
- Cambios en el enfoque o procesos de gestión.
- Cambios derivados de los resultados obtenidos en las actividades de seguimiento y control.
- Nuevas políticas o modificaciones sobre las existentes que afecten al contenido de esta Política.
- Modificación de la estructura organizativa que implique un cambio de funciones en la gestión del riesgo de conducta y cumplimiento.

Como procedimiento de revisión, el responsable de la Política:

- Compartirá el resultado del análisis realizado con el resto de implicados en la gestión del riesgo de conducta y cumplimiento y realizará las modificaciones de la Política que sean necesarias.
- Incluirá un resumen de la revisión efectuada en el apartado "Control de versiones" de la Política.

Control de Versiones

Versión	Fecha	Detalle
AAA.114501	01/10/2024	Versión inicial aprobada por los Administradores
AAA.114502	09/01/2025	Actualización del domicilio postal (apartado 7)
AAA.114503	05/10/2026	Actualización del domicilio postal (apartado 7: C/ Príncipe de Vergara 12, 1º A, 28001 Madrid) y del control de versiones

ANEXO. CONDUCTAS QUE PUEDEN SER COMUNICADAS

1. Cualquier incumplimiento o infracción de los principios establecidos en el Manual de Gobernanza Corporativa.

2. Hechos o conductas que puedan tener transcendencia penal.

   Podrán comunicarse aquellas conductas tipificadas en el Código Penal y los delitos previstos en otras leyes especiales, susceptibles de generar responsabilidad penal para Coventina, tales como:

   Blanqueo de Capitales y Financiación del Terrorismo: aceptar fondos, depósitos, etc. que tengan su origen en la comisión de un delito, o realizar cualquier otro acto para ocultar dicho origen ilícito, o para ayudar a la persona que haya participado en la infracción. Se puede cometer de manera imprudente si se actúa sin la diligencia debida, es decir, no es necesario que el autor quiera y conozca que el delito va a cometerse. Proveer, recolectar o aceptar fondos con la intención de que se utilicen para cometer delitos relacionados con organizaciones y grupos terroristas.

   Ejemplos: ocultar el verdadero origen de los bienes sabiendo que proceden de una actividad delictiva.

   Fraude: afirmación de falsedades o distorsión u ocultación de la verdad para obtener una ventaja financiera ilegal para uno mismo o para una tercera parte.

   Ejemplos: emisión de facturas hinchadas para quedarse con el excedente; fraude crediticio; fraudes con las subvenciones; fraudes con los seguros. Falsificación de documentos. Sustracción de bienes del almacén o la oficina.

   Protección de datos personales: violaciones graves de las normativas destinadas a la protección de los datos personales.

   Ejemplos: compartir datos de clientes y empleados; venta no autorizada de datos especialmente sensibles; abuso continuado y extendido de datos en las comunicaciones por correo electrónico y teléfono.

   Abuso de poder: consiste en aprovecharse de la autoridad que se tiene para extorsionar a otra persona o entidad con el fin de cumplir sus propios intereses.

   Ejemplos: realización de actos de discriminación, utilización de información para beneficio personal o perjudicar a otras personas…

   Corrupción en los negocios: que un directivo, administrador, empleado o colaborador/a, de Coventina por sí o por persona interpuesta, reciba, solicite o acepte un beneficio o ventaja no justificados de cualquier naturaleza, para sí o para un tercero, como contraprestación para favorecer indebidamente a otro en la adquisición o venta de mercancías, o en la contratación de servicios o en las relaciones comerciales. En sentido contrario, la promesa u concesión del beneficio a un/a tercero para la adquisición o venta de productos en las relaciones comerciales.

   Descubrimiento y revelación de secretos de empresa: apoderarse por cualquier medio de datos, documentos ya sean escritos o electrónicos, soportes informáticos u otros objetos que constituyan información confidencial de otra empresa, entidad, etc., para su uso, difusión, revelación, o cesión.

Ejemplos: obtener información secreta de terceros

Estafa: engañar a otro, con ánimo de lucro, para que realice un acto de disposición que le perjudique a él/ella mismo o a un tercero.

Ejemplos: suplantación de identidad de empresas autorizadas

Abuso o acoso sexual: el abuso sexual se refiere a la intrusión física, real o intencionada, de naturaleza sexual, ya sea por la fuerza o bajo condiciones desiguales o coercitivas. El acoso sexual se entiende como conductas de naturaleza sexual que se consideran ofensivas o humillantes, que pueden interferir con las tareas de una persona, que se usan como condicionante para contratar a alguien o que crean un entorno intimidante, hostil u ofensivo.

Ejemplos: agredir a alguien sexualmente, compartir o mostrar imágenes o videos sexuales.

Publicidad engañosa: realizar ofertas o publicidad de productos o servicios, donde se hagan alegaciones falsas o manifiesten características inciertas sobre los mismos, de modo que puedan causar un perjuicio grave y manifiesto a los/las consumidores/as.

Ejemplos: ocultar costes adicionales (impuestos o costes asociados), ocultar información sobre la necesidad de otros productos complementarios

Soborno: ofrecer o entregar a funcionarios, autoridades, organismos y administraciones públicas un regalo o compensación, económica o de cualquier naturaleza, con la intención de obtener un beneficio para Coventina, sea lícito o ilícito.

Ejemplos: Sobornar y aceptar sobornos, pagos de facilitación, extorsión.

Tráfico de influencias: influir igualmente, aprovechándose de cualquier situación derivada de una relación personal, para conseguir una resolución que pueda generar, directa o indirectamente, un beneficio económico para Coventina.

Ejemplo: utilización de contactos en la Administración Pública para obtener contratos públicos, otorgamiento de un permiso o licencia por parte de una autoridad a cambio de un favor.

3. Cualesquiera acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea siempre que:

   Sean infracciones del Derecho de la Unión que entren dentro del ámbito de aplicación de los actos enumerados en el Anexo de la Directiva 2019/1937, relativas a los siguientes ámbitos:

   i) contratación pública; ii) servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo; iii) seguridad de los productos y conformidad; iv) seguridad del transporte; v) protección del medio ambiente; vi) protección frente a las radiaciones y seguridad nuclear; vii) seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales; viii) salud pública; ix) protección de los consumidores; x) protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información.

   Afecten a los intereses financieros de la Unión Europea tal y como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE); o

   Incidan en el mercado interior, tal y como se contempla en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión Europea en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre

sociedades o con prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades.

4. Cualquier otro tipo de irregularidad que pueda implicar responsabilidad para Coventina.