Procedimiento de gestión de informaciones

Sistema interno de información

VERSIÓN 1

NOVIEMBRE 2023

1. Antecedentes

1.1. Introducción

El 21 de febrero de 2023 se publicó en el Boletín Oficial del Estado 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. Con la aprobación de esta ley se incorpora 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.

La referida Ley 2/2023, de conformidad con la Directiva, tiene como finalidad la protección de las personas que en un contexto laboral o profesional detecten determinadas infracciones penales o administrativas graves o muy graves y las comuniquen mediante los canales internos de información que deberán habilitarse al respecto, otorgando una protección adecuada frente a cualquier tipo de represalias.

En cumplimiento de dicha ley, en noviembre de 2023 el Consejo de Administración de **COLONYA, CAIXA D'ESTALVIS DE POLLENÇA** (en adelante "**Colonya**" o la "**Entidad**") ha aprobado su *Política del sistema interno de información y defensa del informante* que tiene como objetivo definir los principios y premisas que regulan dicho sistema, el cual se configura como una herramienta para fortalecer la cultura de la información/comunicación como mecanismo esencial para la prevención, detección y corrección de amenazas al interés público y de incumplimientos normativos, consolidar el marco de supervisión del riesgo de integridad y facilitar el cumplimiento del Código de Conducta y Actuación de la Entidad en general y de su normativa interna en particular.

Así mismo, de acuerdo con el artículo 9 de la Ley 2/2023, el Consejo de Administración de la Entidad debe aprobar el procedimiento de gestión de informaciones.

1.2. Objetivo

El presente *Procedimiento de gestión de informaciones* tiene la finalidad de establecer las previsiones necesarias para que el *Sistema interno de información* de la Entidad y los canales internos de información existentes cumplan con los requisitos establecidos en la Ley 2/2023.

1.3. Ámbito de aplicación

El presente procedimiento tiene carácter corporativo, por lo que es aplicable a los órganos de gobierno, comités, oficinas y departamentos de la Entidad que adaptarán sus principios de actuación, metodologías y procesos a lo descrito en este documento.

El incumplimiento de lo establecido en este procedimiento podrá suponer el ejercicio de la potestad disciplinaria por parte de los órganos internos habilitados para aplicarla.

1.4. Marco normativo

El presente procedimiento se regirá por lo previsto en la normativa aplicable vigente, así como por aquella que la modifique o sustituya en el futuro. A fecha de su elaboración, entre otras, la normativa aplicable vigente es la siguiente:

- Directiva (UE) 2019/1937 del Parlamento Europeo 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.
- 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.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal y sus posteriores modificaciones.
- Circular 1/2011 de la Fiscalía General del Estado, de 1 de junio, relativa a la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica número 5/2010.
- Circular 1/2016 de la Fiscalía General del Estado sobre la responsabilidad penal de la persona jurídica conforme a la reforma del Código Penal efectuada por LO 1/2015.
- Real Decreto-ley 11/2018, de 31 de agosto, de transposición de directivas en materia de prevención del blanqueo de capitales.
- Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales cuyo objeto es adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos.
- Real Decreto Legislativo 4/2015 por el que se aprueba el texto refundido de la Ley del Mercado de Valores.
- Circular 1/2020 de la CNMV por la que se modifican la Circular 5/2013, de 12 de junio, que establece los modelos de informe anual de gobierno corporativo de las sociedades anónimas cotizadas, de las cajas de ahorros y de otras entidades que emitan valores admitidos a negociación en mercados oficiales de valores; y la Circular 4/2013, de 12 de junio, que establece los modelos de informe anual de remuneraciones de los consejeros de sociedades anónimas cotizadas y de los miembros del consejo de administración y de la comisión de control de las cajas de ahorros que emitan valores admitidos a negociación en mercados oficiales de valores.
- Guía de la AEPD sobre la protección de datos en las relaciones laborales. Adicionalmente, esta Política tiene en cuenta otros estándares nacionales e internacionales en la materia, como son:
- Norma ISO 37002 de Sistemas de Gestión de la denuncia de irregularidades.

- Norma ISO 37301 de Sistemas de Gestión de Cumplimiento Normativo.
- Norma UNE 19601 sobre Sistemas de Gestión de Cumplimiento Normativo Penal.
- Norma ISO 37001 de Sistemas de Gestión Antisoborno.

2. Roles y responsables del procedimiento

A continuación, se describen los responsables últimos para llevar a cabo los roles y acciones necesarios para desarrollar, validar, implantar y controlar el presente procedimiento:

Función	Responsables
Petición y revisión	Comité de Dirección
Creación o coordinación	Área de Control Global de Riesgos
Validación	Director de Riesgos
Aplicación	Departamento de Cumplimiento Normativo y Control Interno
Supervisión	Comisión Mixta de Auditoría y Riesgos
Seguimiento y control	Departamento de Auditoría Interna
Firmas y aprobación	Consejo de Administración
Modificaciones y bajas	Consejo de Administración
Archivo y difusión	Área de Organización

3. Identificación de canales de información

El *Sistema interno de información* de la Entidad integra los distintos canales internos de información, lo que permite garantizar en todos ellos que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la Entidad con el objetivo de que sea esta la primera en conocer la posible irregularidad.

3.1. Canal de denuncias

El Canal de Denuncias de la Entidad es la vía principal para posibilitar la presentación de información respecto de posibles infracciones por actos o conductas, presentes o pasadas, que puedan suponer un incumplimiento del Código de Conducta y Actuación u otras normas de conducta relacionadas en la *Política del sistema interno de información y defensa del informante* de la Entidad.

Las comunicaciones pueden presentarse de forma nominativa, es decir, con identificación del informante, o de forma anónima.

Este canal permite la presentación de comunicaciones a través de:

- La Web corporativa accesible a través de *https://colonya.com/es/asistencia/canal-de-denuncias/*.
- Correo electrónico: canaldedenuncias@colonya.es

- Correo postal: Plaça Major, 7, 2º piso; 07460 Pollença, Illes Balears (Att. Departamento de Cumplimiento Normativo y Control Interno).
- Por teléfono al 871 11 71 16 (Departamento de Cumplimiento Normativo y Control Interno).

Las comunicaciones también pueden presentarse verbalmente mediante reunión presencial dentro del plazo máximo de siete días, a solicitud del informante. En estos casos debe dirigirse la petición a través de alguna de las vías de comunicación escritas mencionadas anteriormente.

Las comunicaciones verbales, incluidas las realizadas a través de reunión presencial o telefónicamente, previo consentimiento del informante, serán documentadas:

- a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla, ofreciendo al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación; o
- mediante una grabación de la conversación en un formato seguro, duradero y accesible; en cuyo caso, se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo con lo que establece el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

3.2. Otros canales

A través de los miembros de los órganos de gobierno o empleados de los distintos departamentos u oficinas de Colonya, podrían realizarse comunicaciones por canales distintos al anterior o cuyo/s destinatario/s sean persona/s no responsables de su tratamiento, pero que por su importancia debieran tratarse dentro del *Sistema interno de información*.

En estos casos, el receptor comunicará al informante la opción de utilizar el Canal de Denuncias y, en caso de que no lo quiera utilizar, remitirá inmediatamente la comunicación al Responsable del *Sistema interno de información* a través de la dirección de correo electrónico canaldenuncias@colonya.es, garantizará la confidencialidad de la información recibida, tanto antes como después de su remisión al Responsable del *Sistema interno de información* y deberá cumplir con el resto de las garantías y el marco de gestión establecido en el presente Procedimiento.

3.3. Canal externo de información

Sin perjuicio del acceso a los canales internos detallados 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.

4. Marco de gestión

El presente marco de gestión se basa en los principios y garantías del *Sistema interno de información* de la Entidad, cuyo detalle se encuentra en la *Política del sistema interno de información y defensa del informante*.

Este procedimiento involucra a diversas áreas para asegurar la preservación de la autonomía e independencia en todas las etapas del proceso de gestión de las comunicaciones. Las gestiones se llevarán a cabo de manera personalizada y en colaboración con las partes involucradas, manteniendo un registro documental de todas las acciones realizadas.

A continuación, se muestran las distintas fases del proceso de gestión de las comunicaciones:

4.1. Fase de registro

Cualquier miembro de alguno de los colectivos con acceso al *Sistema interno de información* de la Entidad podrá dirigirse como informante de buena fe a alguno de los canales internos mencionados anteriormente.

El informante deberá facilitar los datos que se estimen necesarios. Si se utiliza el Canal de Denuncias accesible a través de la WEB corporativa de la Entidad, el informante cumplimentará el formulario de obtención de datos disponible. Dicho canal es el mismo independientemente del tipo de infracción y está diseñado para guiar al usuario en los datos a introducir, indicando con un asterisco los campos de cumplimentación obligatoria.

Las comunicaciones, que pueden ser nominativas o anónimas, quedarán registradas.

En el plazo máximo de 7 días el informante recibirá un acuse de recibo, salvo que:

- ello pueda poner en peligro la confidencialidad de la comunicación,
- el informante expresamente haya renunciado a recibir comunicaciones relativas a la investigación,
- la Entidad considere razonablemente que el acuse de recibo de la información comprometería la protección de la identidad del informante.

En su caso, dicho acuse de recibo incluirá la dirección de correo electrónico del Canal para poder contactar con el Responsable del *Sistema interno de información* en caso de que el receptor del acuse de recibo no sea el destinatario correcto.

El informante tiene la opción de proporcionar información adicional y documentación relacionada con la comunicación después de su presentación, ya sea de forma voluntaria o a solicitud del Responsable del *Sistema interno de información*. Los nuevos hechos y documentos presentados serán tomados en cuenta en el proceso de gestión.

Las comunicaciones presentadas por cualquier vía, ya se trate de comunicaciones realizadas por el propio informante como aquellas remitidas al Responsable del *Sistema interno de información* por parte del canal o del receptor no responsable de la gestión, serán incorporadas por el Responsable del *Sistema interno de información* al *Registro de informaciones*, garantizando, en todo caso, los requisitos de confidencialidad previstos en la Ley 2/2023.

El *Registro de informaciones* estará contenido en una base de datos segura y de acceso restringido exclusivamente al personal de la Entidad convenientemente autorizado, en la que se registrarán todas las comunicaciones recibidas, cumplimentando como mínimo los siguientes datos:

a) Fecha de recepción.

b) Código de identificación.

c) Admisión (si/no)

d) Actuaciones desarrolladas.

e) Medidas adoptadas.

f) Fecha de cierre.

Los datos personales relativos a las informaciones recibidas y a las investigaciones internas solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con la Ley 2/2023. En ningún caso podrán conservarse los datos por un período superior a diez años.

4.2. Fase de análisis

Registrada la información, las comunicaciones presentadas serán objeto de un **análisis de admisibilidad**. Quedan excluidas del alcance del *Sistema interno de información* las comunicaciones que:

- No queden comprendidas dentro del ámbito material de la Ley 2/2023 y/o que no versen sobre hechos/conductas sobre irregularidades que puedan suponer infracciones de la normativa interna de aplicación a la Entidad según lo dispuesto en la *Política del sistema interno de Información y defensa del informante*.
- Sean presentadas por un colectivo sin acceso al *Sistema interno de información*, como son las reclamaciones de clientes que deberían realizarse a través del Servicio de Atención al Cliente.
- Cuando los hechos relatados carezcan de toda verosimilitud.
- Se basen en información pública.
- Carezcan claramente de fundamento o existan indicios razonables, según la evaluación de la Entidad, de que la información se ha obtenido mediante la comisión de un delito. En este último caso se enviará al Ministerio Fiscal un informe detallado de los hechos que se consideren constitutivos de delito.

- Estén relacionadas con disputas o conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación.
- Se fundamenten en meros rumores y/o no estén fundadas en sospechas o indicios concretos.
- Se basen en documentación que no se ha aportado y que no es accesible para la Entidad.
- Estén relacionadas con actuaciones o conductas que ya están siendo investigadas por la autoridad competente (policía, justicia, etc.).
- No contengan 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, la Entidad, notificará la resolución de manera motivada.

En cualquier caso, el Responsable del *Sistema interno de información* podría admitir una comunicación que, aun siendo inadmisible según los criterios anteriores, revelara hechos o conductas que a su juicio requieran de un mayor análisis a través del *Sistema interno de información*.

Aunque no sea un requisito para su admisión, las comunicaciones deberían ir acompañadas de documentos justificativos u otros medios de prueba.

Así mismo, el Responsable del *Sistema interno de información* para analizar la admisibilidad de las comunicaciones podrá requerir la colaboración de un experto interno o externo y, en su caso, solicitar al informante aclaraciones o información adicional.

Siempre que sea posible, el Responsable del *Sistema interno de información* comunicará al informante la decisión de admisión/inadmisión:

- Si la comunicación no se admite, se dará el expediente por concluido .
- Si es admitida, se continuará con el análisis y el inicio de las comunicaciones con las partes interesadas y el cumplimiento de los requisitos en materia de protección de datos personales, dejando constancia en el *Registro de informaciones* de las actuaciones internas realizadas, garantizando siempre la confidencialidad de la información.

  Siempre que no ponga en peligro el curso de la investigación y en un plazo máximo de 2 meses desde su registro, se comunicará lo antes posible la recepción de la comunicación a las personas denunciadas y/o afectadas y se dará traslado al equipo/persona de auditoría interna que vaya a realizar la investigación según se indica el apartado 4.3.

  En todo caso, la comunicación a las personas denunciadas y/o afectadas incluirá:

  - la recepción de la comunicación y la fecha,
  - las conductas/hechos que se atribuyen,

- el equipo/persona responsable de su gestión,
- el tratamiento que se realizará de sus datos de carácter personal, y
- El derecho de presentar alegaciones por escrito.

En ningún caso se comunicará a las personas denunciadas y/o afectadas la identidad del informante ni se dará acceso a la comunicación.

4.3. Fase de investigación

El equipo/persona responsable de la investigación normalmente formará parte del Departamento de Auditoría Interna, sin perjuicio de que, según la naturaleza de los hechos o conductas objeto de la comunicación, deban intervenir otras áreas o departamentos especializados (Departamento de Asesoría Jurídica, Departamento de Recursos Humanos, etc.) o expertos externos.

El Responsable del Sistema interno de información se reunirá con el equipo investigador y le trasladará toda la documentación disponible, facilitando la identidad del informante si es un dato imprescindible para el curso de la investigación y siempre con el consentimiento previo del propio informante.

La investigación se llevará a cabo lo antes posible, cumpliendo las garantías previstas en la *Política del sistema interno de información y defensa del informante* y, en cualquier caso, garantizando para todas las personas afectadas (se hayan o no identificado inicialmente en la comunicación):

- el respeto a la presunción de inocencia y al honor,
- el derecho a ser oída en cualquier momento y a exponer su versión de los hechos,
- el derecho a presentar alegaciones por escrito y a aportar aquellos medios de prueba que considere adecuados y pertinentes,
- el derecho a ser informadas de las acciones u omisiones que se le atribuyen,
- la preservación de su identidad y la confidencialidad de los hechos y datos del procedimiento.

Para comprobar la verosimilitud de los hechos relatados en la comunicación, el procedimiento de investigación podrá incluir:

- Reuniones con el informante (siempre que sea posible) para obtener aclaraciones o información adicional.
- Entrevistas o reuniones con los departamentos y/o las personas afectadas directa o indirectamente.
- Análisis de datos y obtención de información.
- Petición de pruebas periciales a profesionales internos o externos a la Entidad.
- Otras diligencias de investigación o prueba que se consideren pertinentes.

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

Se aplicarán las medidas de protección que se estimen necesarias antes y durante la investigación, tales como salvaguardar la separación e independencia entre el equipo investigador y las personas investigadas.

4.4. Fase de resolución

Con las evidencias disponibles y las conclusiones de la fase de investigación, en el plazo de 3 meses desde la recepción de la comunicación, el Responsable del *Sistema interno de información* resolverá sobre el cumplimiento/incumplimiento de la normativa respecto los hechos/conductas objeto de comunicación, y así se comunicará a las partes involucradas a la mayor celeridad posible.

No obstante, el plazo de resolución se extenderá hasta los 6 meses si las circunstancias específicas del caso justifican que la investigación se demore; en cuyo caso se informará a las partes involucradas y se continuará con su gestión hasta su efectiva resolución, aplicando en cualquier caso las medidas establecidas en la normativa de protección de datos.

Si la persona que ha cometido la infracción es un empleado de la Entidad, el Responsable del *Sistema interno de información* remitirá el expediente al Departamento de Recursos Humanos, para que adopte las medidas disciplinarias o sancionadoras oportunas. 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.

5. Protección de datos personales

El *Sistema interno de información* de la Entidad garantiza la confidencialidad y la protección de datos personales de las personas involucradas en las comunicaciones durante todo el proceso de gestión de las mismas.

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 la misma y en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

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.

Cuando se obtengan directamente de los interesados sus datos personales se les facilitará la información a que se refieren los artículos 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 11 de la Ley Orgánica 3/2018, de 5 de diciembre.

A los informantes se les informará, de forma expresa, 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.

El acceso a los datos personales contenidos en el *Sistema interno de información* quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente a:

a) El Responsable del *Sistema interno de información* y a quien lo gestione directamente.

b) El responsable del Departamento de Recursos Humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.

c) El responsable del Departamento de Asesoría Jurídica de la Entidad si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.

d) Los encargados del tratamiento que eventualmente se designen.

e) El delegado de protección de datos (DPD) de la Entidad.

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.

En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones que han sido objeto de comunicación, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la Ley 2/2023.

Si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de los mismos.

Los datos personales 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. Si la comunicación no es admitida, se procederá a la supresión de los datos, salvo que la inadmisión se produjera por la falta de veracidad de la información facilitada 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 meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, se suprimirán 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 prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

Los empleados y terceros deberán ser informados acerca del tratamiento de datos personales en el marco del *Sistema interno de información*.

6. Medidas de protección al informante

Los informantes de comunicaciones admitidas tendrán **derecho a protección** siempre que concurran las circunstancias siguientes:

- Tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación, aun cuando no aporten pruebas concluyentes, y que la citada información entra dentro del alcance del *Sistema interno de información*, de acuerdo con el ámbito de aplicación de la Ley 2/2023.
- La comunicación se haya realizado conforme a los requerimientos previstos en la Ley 2/2023 y recogidos en la *Política del sistema interno de información y defensa del informante* y en el presente procedimiento.

También tendrán derecho a protección las personas que hayan comunicado información sobre acciones u omisiones potencialmente irregulares de forma anónima pero que posteriormente hayan sido identificadas.

De acuerdo con el artículo 36 de la Ley 2/2023, se prohíben expresamente los actos constitutivos de represalia[1], incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación en el ámbito del *Sistema interno de información.*

Los informantes no incurrirán en responsabilidad respecto de la adquisición o el acceso a la información que es comunicada o revelada públicamente, siempre que dicha adquisición o acceso no constituya un delito.

Así mismo, conforme al artículo 37 de la Ley 2/2023, los informantes de comunicaciones admitidas dentro del *Sistema interno de información* tendrán acceso a las siguientes **medidas de apoyo**:

a) Información y asesoramiento completos e independientes, que sean fácilmente accesibles para el público y gratuitos, sobre los procedimientos y recursos disponibles, protección frente a represalias y derechos de la persona afectada.

[1] Se entiende por represalia cualesquiera actos u omisiones que estén 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, o por haber realizado una revelación pública. Entre otras, se consideran represalias a efectos de la Ley 2/2023: suspensión del contrato de trabajo, despido o extinción de la relación laboral, degradación o denegación de ascenso, terminación anticipada de contratos de bienes o servicios, daños económicos o reputacionales, acoso, intimidación, inclusión en listas negras, denegación de permisos o formación, discriminación o trato desfavorable o injusto.

b) Asistencia efectiva por parte de las autoridades competentes ante cualquier autoridad pertinente implicada en su protección frente a represalias, incluida la certificación de que pueden acogerse a protección al amparo de la Ley 2/2023.

c) Asistencia jurídica en los procesos penales y en los procesos civiles transfronterizos de conformidad con la normativa comunitaria.

d) Apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la Autoridad Independiente de Protección del Informante, A.A.I. tras la valoración de las circunstancias derivadas de la presentación de la comunicación.

7. Firmas y aprobaciones

El presente procedimiento ha sido:

Realizado por:	Área de Control Global de Riesgos	Noviembre 2023
Revisado por:	Director de Riesgos	Noviembre 2023
Validado por:	Comité de Dirección	02-11-2023
Aprobado por:	Consejo de Administración	20-11-2023
Publicado en la:	Web corporativa	Noviembre 2023

8. Plan de seguimiento y control del cumplimiento

Una vez que el procedimiento está implantado, se tiene que realizar un seguimiento continuado del mismo para comprobar su correcto cumplimiento.

El Comité de Dirección y el Consejo de Administración de la Entidad se asegurarán de que este procedimiento esté efectivamente implantado.

El control de su cumplimiento correrá a cargo del Departamento de Auditoría Interna.

Las conclusiones del seguimiento deben conducir a acciones cuyo principal objetivo sea incrementar el grado de cumplimiento o mejorar el impacto del procedimiento en la Entidad o en sus empleados.

Los cambios propuestos y la razón por la que se formula la propuesta de modificación serán comunicados para su validación al Director de Riesgos. Una vez se hayan validado y aprobado los cambios por parte del Consejo de Administración se realizará la modificación y actualización del presente documento.

La tipología de los controles o revisiones pueden dividirse en:

- Revisiones sistemáticas o periódicas: La Comisión Mixta de Auditoría y Riesgos dará las instrucciones oportunas al Departamento de Auditoría Interna para que incluya en su planificación de trabajo la revisión y control del cumplimiento de este procedimiento.

- Revisiones sintomáticas: En caso de que haya indicios de incumplimiento del presente procedimiento se reportarán al Departamento de Auditoría Interna para su revisión y control.
- Revisiones a petición: peticiones de cambios procedentes de los impactados por el procedimiento. En estos casos se evaluará la necesidad de modificar el procedimiento.

9. Control del documento

9.1. Modificaciones y bajas

Este procedimiento irá adaptándose a los cambios normativos y a los de la propia organización. Por ello será revisada con una frecuencia mínima anual por parte del responsable del Departamento de Cumplimiento Normativo y Control Interno y, en caso de que lo estime pertinente, propondrá modificaciones que se elevarán al Consejo de Administración para su aprobación.

En concreto, las causas de modificación y actualización pueden ser:

- Cambios derivados del proceso de seguimiento y control.
- Cambios en los objetivos y estrategia de negocio.
- Cambios en el enfoque o procedimientos de gestión.
- Nuevas políticas o modificaciones sobre las existentes que afecten al contenido del presente procedimiento.
- Modificación de los procesos o procedimientos.
- Modificación de la estructura organizativa que implique un cambio de funciones en la gestión de informaciones.
- Cambios en el marco normativo.

Cualquier modificación o baja del presente procedimiento debe ser validada por el Director de Riesgos, revisada por el Comité de Dirección y aprobada por el Consejo de Administración, previo informe favorable de la Comisión Mixta de Auditoría y Riesgos.

9.2. Archivo y difusión

El documento original del presente procedimiento se halla archivado en G:\200. Politiques i procediments\200.22 Política del sistema interno de información y defensa del informante.

La difusión del procedimiento entre los empleados de la Entidad se realizará mediante la publicación de una circular interna y su puesta a disposición en formato PDF en la Intranet de la Entidad.

Así mismo, el presente procedimiento estará a disposición de los terceros descritos en el apartado 1.2., mediante su publicación en un apartado separado y fácilmente identificable de la página web corporativa de Colonya proporcionando una información adecuada y suficiente sobre los distintos aspectos de este procedimiento.

9.3. Control de versiones

A continuación, se detalla el control de las versiones:

Versión	Fecha aprobación	Control
1	20-11-2023	Versión inicial

9.4. Referencia a otros documentos internos

El presente procedimiento desarrolla el contenido de la *Política del sistema interno de información y defensa del informante* de la Entidad.

Además, dicha política y el presente procedimiento se complementan con los siguientes documentos internos relacionados con la gestión del riesgo de cumplimiento y conducta:

- Código de Conducta y Actuación
- Manual de prevención de riegos penales
- Política de Gestión de Conflictos de Interés
- Reglamento Interno de Conducta en el ámbito del Mercado de Valores
- Manual de gestión y control de compras