

Política del Sistema Interno de Información y Procedimiento de Gestión de Informaciones

Grupo CIMD

Septiembre 2026

HISTÓRICO DE VERSIONES

Versión	Fecha de Elaboración	Autor	Descripción de Cambios
1.0	Noviembre 2023	Órgano de Vigilancia y Control para la Prevención de Delitos	Versión original aprobada por los Órganos de Administración del Grupo CIMD
2.0	Mayo 2024	Órgano de Vigilancia y Control para la Prevención de Delitos	Incorporación de Intermoney Capital, S.G.E.I.C, S.A.
3.0	Noviembre 2025	Órgano de Vigilancia y Control para la Prevención de Delitos	Adaptación del ámbito de aplicación
4.0	Septiembre 2026	Órgano de Vigilancia y Control para la Prevención de Delitos	Actualización de los miembros del Órgano de Control y Vigilancia

Contenido

1. Introducción	4
2. Ámbito de aplicación	4
3. Principios y garantías del Sistema Interno de Información	5
4. Canales de Denuncias	7
5. Procedimiento de Gestión de Informaciones	8
6. Medidas de protección	10
7. Protección de datos personales	11
8. Responsable del Sistema Interno de Información	12
9. Revisión y publicación de la Política del Sistema Interno de Información y del Procedimiento de Gestión de Informaciones	12

1. Introducción

El presente documento establece la política necesaria para que el Sistema Interno de Información y el procedimiento de gestión de informaciones cumpla con los requisitos establecidos en 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 (en adelante, la Ley 2/2023), que transpone al ordenamiento jurídico 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 presente **Política del Sistema Interno de Información y Procedimiento de Gestión de Informaciones** tiene por finalidad definir los principios que regulan el sistema interno de información y las previsiones establecidas para el correcto tratamiento de las informaciones recibidas en el marco de dicho sistema, y de esa manera otorgar una protección adecuada frente a las represalias que puedan sufrir las personas físicas que en un contexto laboral o profesional informen de alguna de las acciones u omisiones que se enumeran en el artículo 2 de la Ley 2/2023.

2. Ámbito de aplicación

Corretaje e Información Monetaria y de Divisas, S.A. (en adelante, “CIMD, SA”), es la empresa matriz del Grupo CIMD, un grupo financiero independiente de intermediación, consultoría, titulización y gestión en mercados de valores y energía del sur de Europa.

La presente Política resulta de aplicación a todas las filiales de CIMD, SA establecidas en España, y, en su caso, a las filiales de estas mismas, que, en cada momento, formen parte del Grupo CIMD.

Se aprueba la presente Política por el Consejo de Administración de la sociedad matriz CIMD, SA, así como por los Órganos de Administración de las empresas españolas que formen parte del Grupo CIMD, afectando a todos sus administradores y trabajadores con independencia de su cargo, responsabilidad o nivel jerárquico, abarcando cualquier área o departamento y ámbito territorial o geográfico en donde desempeñen sus funciones. Las personas que ostenten responsabilidad deben encargarse de que las personas que estén a su cargo conozcan y cumplan la presente Política.

La aplicación del presente documento en las filiales fuera de España debe ir precedida de un análisis de su contenido en relación con los requerimientos regulatorios de la jurisdicción de que se trate, dependiendo dicha aplicación de la normativa local del país donde se encuentra constituida la filial.

El Sistema Interno de Información integra diferentes mecanismos de comunicación a través de los cuales se podrá informar de las siguientes materias:

- Acciones u omisiones que puedan constituir infracciones penales o administrativas graves o muy graves.
- Acciones u omisiones que puedan ser constitutivas de infracciones del Derecho de la Unión Europea con las consideraciones establecidas en la Ley 2/2023.
- Vulneraciones del derecho laboral en materia de seguridad y salud en el trabajo que puedan constituir infracciones penales o administrativas graves o muy graves.

Con independencia de la posibilidad de recibir otras denuncias de otros ámbitos normativos, única y exclusivamente quedarán amparadas bajo las medidas de protección que se establecen en la Ley 2/2023 aquellas comunicaciones recogidas en el artículo 2 de la misma.

No obstante, el artículo 10.b) de la Ley 2/2023 indica que estarán obligadas a disponer de un Sistema Interno de Información aquellas personas jurídicas que entren en el ámbito de aplicación en materia de prevención de blanqueo de capitales o financiación del terrorismo. Por lo tanto, quedarán bajo el Sistema Interno de Información las denuncias y/o comunicaciones que un informante presente sobre esta materia.

Las personas con acceso al Sistema Interno de Información del Grupo CIMD y sujetas a las medidas de protección de la Ley 2/2023 son:

- Empleados y miembros de los Órganos de Administración de las sociedades del Grupo CIMD.
- Becarios y trabajadores en periodos de formación.
- Agentes.
- Colaboradores, proveedores y cualquier persona que trabaje para o bajo la supervisión y dirección de dichos colaboradores y proveedores.
- Accionistas.
- Exempleados.
- Candidatos a un puesto de trabajo.

3. Principios y garantías del Sistema Interno de Información

El cumplimiento con las leyes y normativas internas de aplicación es responsabilidad de todos los integrantes del Grupo CIMD. En este sentido, concurre el deber de informar sobre cualquier hecho que pueda constituir delito e irregularidad.

Principio de Legalidad

La base esencial en que se asienta el Sistema Interno de Información es el principio de la legalidad, incorporando y transcribiendo los principios y disposiciones de la Ley 2/2023.

En concreto, el Sistema Interno de Información se regirá por el derecho de información, derecho de defensa, derecho a la presunción de inocencia del denunciado y el derecho al honor de todas las personas sobre las que se presente una denuncia y/o que se vean afectadas. El denunciado tiene derecho a conocer las acciones u omisiones que se le atribuyen mediante comunicación sucinta de los hechos y a ser oído en cualquier momento, en la forma en la que se considere adecuado para garantizar el buen fin de la investigación.

Confidencialidad y anonimato

El Sistema Interno de Información garantizará la confidencialidad de la identidad del informante y de cualquier tercero mencionado en las comunicaciones, de la información comunicada y de las actuaciones que se desarrollen en la gestión y tramitación de la misma. El sistema implantado vela por que las personas implicadas en la tramitación e investigación de las comunicaciones actúen con la máxima discreción sobre los hechos que conozcan por razón de su cargo o función.

El acceso a la información se encuentra restringido a las personas con potestad de gestión según se define en el presente documento, quedando expresamente prohibido divulgar cualquier tipo de información sobre las comunicaciones.

Las comunicaciones enviadas al Sistema Interno de Información pueden ser tanto nominativas (con identificación del informante) como anónimas.

En el caso de que la comunicación remitida sea anónima queda prohibido el rastreo y trazabilidad de dichas comunicaciones.

Ausencia de represalias: la protección al informante

La ausencia de represalias, la protección al informante u otras personas involucradas o relacionadas con el mismo, siempre que las comunicaciones sean realizadas de buena fe y con arreglo a la normativa, asumiendo la protección del informante, es elemento esencial de esta Política. Se prohíbe expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación.

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, intimidación, acoso, discriminación, o trato desfavorable o injusto.

Los informantes no incurrirán en responsabilidad respecto del acceso a la información que es comunicada o revelada públicamente, siempre que dicho acceso no constituya un delito. El informante de las infracciones previstas en el apartado 2, accederán a las medidas de apoyo establecidas en el artículo 37, de la Ley 2/2023.

Independencia e imparcialidad

Se actuará en todo momento con independencia e imparcialidad y con el máximo respeto a la legislación y normativa interna. Las denuncias serán tramitadas siempre de manera equitativa, íntegra, objetiva, independiente y honesta.

Transparencia y accesibilidad

La información relativa al Sistema Interno de Información se encuentra de una forma clara y fácilmente accesible, y con publicidad suficiente sobre su uso y principios y garantías rectores,

en un apartado separado y fácilmente identificable en la página web corporativa del Grupo CIMD. La información facilitada debe atender a criterios de veracidad y buena fe, evitando proporcionar información confusa, falsa o carente de toda fidelidad. Cualquier incumplimiento de lo dispuesto en la presente Política puede conllevar la aplicación de medidas sancionadoras.

Trazabilidad y seguridad

Las comunicaciones remitidas a través del Sistema Interno de Información, y sometidas a lo dispuesto en la presente Política, serán registradas y tramitadas de acuerdo con la normativa, preservando la integridad de la información remitida. En la tramitación de los expedientes de denuncia se respetará el derecho de todas las personas que intervengan a que sus datos personales e información de carácter privado sean tratados conforme a la legislación de datos de carácter personal que resulte en cada caso de preceptiva aplicación.

Buena fe

De acuerdo con lo establecido en la Ley 2/2023, las comunicaciones presentadas deben remitirse a través del Sistema Interno de Información siempre de buena fe.

Se considerará que las comunicaciones remitidas son de mala fe cuando hayan suplantado la identidad del informante o hechos que se saben inciertos o involucran a personas que no han tenido relación con tales hechos, aun siendo estos ciertos.

4. Canales de Denuncias

A continuación, se enumeran los distintos tipos de canales de información:

1. Canales internos:

El Canal de Denuncias es el cauce preferente para informar sobre las acciones u omisiones previstas por la Ley 2/2023, que garantiza de manera efectiva la infracción de actos o conductas sobre la aplicación de la Política del Sistema Interno de Información y del Procedimiento de Gestión de Informaciones, evitando cualquier riesgo de represalia sobre la persona que denuncia.

Este Canal permite la presentación de comunicaciones escritas a través de las siguientes vías, pudiendo presentarse bien de forma anónima, o bien con identificación del informante:

- Plataforma informática ubicada en la página web del Grupo CIMD, accesible en la siguiente ubicación: <https://www.grupocimd.com/canal-de-denuncias/>
- Correo electrónico: organovigilanciaycontrol@grupocimd.com
- Dirección de correo postal dirigido al Órgano de Vigilancia y Control, Príncipe de Vergara 131, 3ª Planta, 28002 Madrid.

Los informantes asimismo pueden realizar una denuncia de forma verbal, solicitando al Órgano de Vigilancia y Control el envío de la denuncia por correo electrónico adjuntando un fichero de mensajería de voz.

El informante por otro lado podrá solicitar una reunión presencial mediante comunicación escrita a través de los canales anteriormente indicados, que tendrá lugar en un plazo no superior a siete días desde la solicitud. Dicha reunión quedará documentada de alguna de las maneras siguientes, previo consentimiento del informante: i) mediante una grabación de la conversación en un formato seguro, duradero y accesible, o ii) a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla. Sin perjuicio de los derechos que le corresponden de acuerdo a la normativa sobre protección de datos, se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

2. Otros canales:

Dado que las sociedades que forman el Grupo CIMD cuentan con otros canales de comunicación, entre los que se encuentra la dirección de correo electrónico: consultasprevencionacoso@grupocimd.com, que facilitan la posibilidad de remitir denuncias, quejas y/o reclamaciones de otros ámbitos normativos, única y exclusivamente quedarán amparadas bajo las medidas de protección que se establecen en la Ley 2/2023 aquellas comunicaciones recogidas en el artículo 2 de la misma.

En caso de que el informante comunique una irregularidad por canales distintos al Canal de Denuncias y la persona receptora de dicha comunicación detectase que la denuncia es susceptible de incluirse en el ámbito del Sistema Interno de Información, ésta deberá poner en conocimiento del informante la existencia del Canal de Denuncias para que proceda a su presentación a través de dicho canal.

3. Canal externo de información - Autoridad Independiente de Protección del Informante (A.A.I.):

Con independencia del establecimiento de canales de información internos, toda persona física podrá informar ante la Autoridad Independiente de Protección del Informante, A.A.I, o ante las autoridades u organismos autonómicos correspondientes, de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación de la Ley 2/2023, ya sea directamente o previa comunicación hecha al Canal de Denuncias.

5. Procedimiento de Gestión de Informaciones

Recepción y registro

Cualquier persona identificada en el apartado 2 del presente documento con acceso al Sistema Interno de Información del Grupo CIMD podrá dirigir la comunicación a alguno de los canales internos anteriormente identificados.

El informante deberá facilitar los datos que se estimen necesarios.

En el caso de comunicaciones presentadas por otras vías distintas de la plataforma informática, del correo electrónico, del correo postal o mediante reunión presencial, ya se trate de comunicaciones realizadas por el propio informante como aquellas remitidas al Responsable del Sistema por parte de una persona receptora de la denuncia y no responsable de la gestión, serán

incorporadas al Canal de Denuncias una vez obtenida la información y documentación facilitada por el informante.

En el plazo máximo de siete días naturales se deberá enviar por parte del Responsable del Sistema Interno de Información acuse recibo de la comunicación al informante, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.

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. El formato utilizado para mantener contacto depende de las necesidades del caso y atendiendo al canal interno receptor de la comunicación, siendo recomendable que las comunicaciones estén soportadas por medio de pruebas documentales.

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 en 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.

Análisis de la denuncia: admisión o inadmisión

Las comunicaciones presentadas serán objeto de un análisis de admisibilidad, quedando excluidas del alcance del Sistema Interno de Información las que:

- No queden comprendidas dentro del ámbito material de la Ley 2/2023.
- Sean presentadas por un colectivo sin acceso al Sistema Interno de Información.
- Hayan sido inadmitidas por algún canal interno de información.
- Versen sobre hechos disponibles para el público (información pública).
- Se encuentren vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación o revelación.
- Se fundamenten en meros rumores y/o no estén fundadas en sospechas o indicios concretos o determinados.
- Versen específicamente sobre el contenido de un fichero/documento no accesible para las sociedades del Grupo CIMD identificadas en la denuncia y no aportado en la comunicación.
- Sean relativas a hechos/conductas que se encuentren en sede policial, administrativa inspectora y/o judicial.

No obstante, el Responsable del Sistema Interno de Información 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.

El análisis de admisibilidad será realizado por el Responsable del Sistema Interno de Información, debiendo de comunicar al informante de dicho análisis. El Responsable del Sistema Interno de Información puede contar con expertos externos en aras de reforzar la independencia, la objetividad y el respeto a las garantías que ofrece el Sistema Interno de Información.

Investigación de la denuncia

La investigación se llevará a cabo de acuerdo con los procedimientos, principios y garantías previstas en la presente Política y, en cualquier caso, garantizando los derechos que corresponden a las personas afectadas.

El procedimiento de investigación podrá incluir cualquier investigación o prueba que sean pertinentes y útiles, bajo un criterio de proporcionalidad para que sean lo menos gravosas posibles con relación a la posición jurídica de la persona afectada.

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.

Conclusión

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

El plazo máximo para dar respuesta a las actuaciones de investigación no podrá ser superior a tres meses a contar desde la recepción de la comunicación o salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, este podrá extenderse hasta un máximo de otros tres meses adicionales.

Si durante la fase de admisión o investigación los hechos denunciados pudieran ser indiciariamente constitutivos de delito, con carácter inmediato, se remitirá la información al Ministerio Fiscal, y en el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

6. Medidas de protección

Las personas que comuniquen o revelen infracciones previstas en apartado 2 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 o revelación, aun cuando no aporten pruebas concluyentes, y que la citada información entra dentro del ámbito de aplicación de esta Ley.
- La comunicación o revelación se haya realizado conforme a los requerimientos previstos en la Ley 2/2023.

También gozarán de la misma protección las personas que hayan comunicado información sobre acciones u omisiones de forma anónima y que posteriormente hayan sido identificadas.

Se excluye expresamente de la protección a las personas excluidas en el apartado 5 “*Análisis de la denuncia: admisión o inadmisión*”.

7. Protección de datos personales

Todas las actuaciones que se desarrollen en el marco de la presente Política se llevarán a cabo cumpliendo con la normativa de protección de datos vigente.

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 registrarán 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.

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 y a quien lo gestione.
- El Director de Recursos Humanos, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.
- El responsable de Asesoría Jurídica, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.
- 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 una de las compañías del Grupo CIMD 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 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.

Las personas con acceso al Sistema Interno de Información recogidas en el apartado 2 del presente documento serán informadas acerca del tratamiento de datos personales.

8. Responsable del Sistema Interno de Información

Los Órganos de Administración de las compañías del Grupo CIMD han designado como Responsable único del Sistema Interno de Información al Órgano de Vigilancia y Control del Área de Compliance Penal, encargado de su gestión.

El citado Órgano está compuesto por Doña Beatriz Senís Gilmartín y Doña María Aguirre Rodríguez.

Dicho Responsable, como órgano colegiado, actuará con autonomía e independencia de cualesquiera otros órganos, comités o comisiones de las entidades del Grupo CIMD.

9. Revisión y publicación de la Política del Sistema Interno de Información y del Procedimiento de Gestión de Informaciones

Se establece un programa de revisión de la Política del Sistema Interno de Información y del Procedimiento de Gestión de Informaciones con el objetivo de identificar potenciales áreas de mejora, o ante posibles cambios en la normativa vigente.

El responsable de dicha revisión será el Órgano de Vigilancia y Control.

El Órgano de Vigilancia y Control, asimismo, será responsable de la accesibilidad a este documento a través de su publicación tanto en la web corporativa del Grupo CIMD, como en la Intranet Corporativa en su apartado de Políticas.