REGLAMENTO DEL SISTEMA INTERNO DE INFORMACIÓN DE VASCO GROUP

DEFINICIONES CLAVE:

Canales internos: Mecanismos habilitados por la empresa (correo, plataforma web, teléfono, presencial) para la presentación de las comunicaciones.

Canales externos: Autoridades públicas competentes para recibir denuncias sobre irregularidades, incumplimientos legales o delitos, cuando sea necesario derivar información fuera del ámbito interno.

Conflicto de interés: Situación en la que el Responsable del Sistema Interno de Información, instructor/a o cualquier persona involucrada en la investigación podría verse influida por relaciones personales, jerárquicas o económicas que comprometan su imparcialidad.

Datos personales y confidencialidad: Toda información relativa a personas identificadas o identificables que se trate en el Sistema Interno de Información, cuya protección se garantizará según la normativa aplicable (Reglamento General de Protección de Datos y Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales).

Persona informante: Cualquier persona que, dentro o fuera de VASCO Group, comunique de buena fe información sobre posibles infracciones legales, éticas o normativas.

Persona denunciada: Persona contra la que se dirige una comunicación a través del Sistema Interno de Información.

Responsable del Sistema Interno de Información: Persona designada para supervisar y garantizar el correcto funcionamiento del Sistema interno de información.

Sistema Interno de Información: Conjunto de mecanismos, canales y procedimientos establecidos para recibir, tramitar e investigar denuncias de irregularidades. Forman parte del Sistema, el Responsable del Sistema Interno de Información y el presente reglamento.

ÍNDICE

1. Objeto

Este reglamento regula el funcionamiento del Sistema Interno de Información de VASCO Group, de conformidad con 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, Ley 2/2023), así como con la normativa aplicable en materia de protección de datos, prevención de delitos y blanqueo de capitales.

El Sistema Interno de Información es un sistema común a todas las sociedades adheridas de VASCO Group, diseñado para centralizar la recepción, tramitación e investigación de comunicaciones sobre conductas irregulares, garantizando la confidencialidad, imparcialidad y protección de las personas informantes, sin que ello limite la independencia de cada sociedad para asumir su responsabilidad legal y operativa sobre los hechos que le afecten.

Las sociedades de VASCO Group adheridas al Sistema Interno de Información son las siguientes:

- IN SIDE LOGISTICS VALENCIA S.L., NIF B97529507
- IN SIDE LOGISTICS CANARIAS S.L.U., NIF B76774421
- IN SIDE LOGISTICS CARTERA S.L., NIF B56877731
- IBERIAN LOGISTICS S.L., NIF B95337937
- VASCO CATALANA DE CONSIGNACIONES S.A., NIF A48058242
- VASCO SHIPPING SERVICES S.L., NIF B48818983
- INTERMODAL FORWARDING S.L., NIF B67061648
- VASCO SERVICIOS COMPARTIDOS S.L., NIF B22496145
- VASCOTECH S.L., NIF B98959091
- VASCO SUPPLY CHAIN S.L., NIF B70841713

2. Propósito del Sistema Interno de Información

El Sistema Interno de Información de VASCO Group se concibe como un instrumento de aprendizaje organizacional y un elemento central de la estrategia de cumplimiento, diseñado para detectar y gestionar de manera temprana conductas o situaciones que puedan infringir la normativa aplicable.

Mediante la identificación y tramitación de las comunicaciones recibidas, el sistema permite a cada sociedad:

- Detectar infracciones legales antes de que dañen la reputación de la organización o se consoliden como prácticas habituales.
- Adoptar medidas correctoras eficaces para poner fin a las conductas detectadas, reparar sus efectos y prevenir su reiteración.
- Reforzar el mensaje de que todas las personas de la organización son guardianas de la legalidad y de las buenas prácticas.

- Fomentar una cultura de cumplimiento y transparencia, consolidando un entorno de trabajo basado en la responsabilidad compartida.

En consecuencia, el Sistema Interno de Información no constituye un mero canal de comunicación interna, sino el pilar central de la estrategia de cumplimiento de VASCO Group y de las diversas sociedades, permitiendo que la gestión de las comunicaciones sea común, sin interferir en la autonomía ni en las decisiones de cada sociedad.

3. Tipos de comunicaciones y hechos a reportar

El Sistema Interno de Información es un mecanismo que permite a cualquier persona del entorno laboral o profesional de las empresas de VASCO Group comunicar de forma confidencial información sobre infracciones previstas en el artículo 2 de la Ley 2/2023:

- Acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea.
- Acciones u omisiones que puedan constituir infracciones penales, así como infracciones administrativas graves o muy graves.
- Acciones u omisiones que puedan constituir infracciones de los planes y medidas frente al acoso laboral y frente al acoso sexual y por razón de sexo establecidas en las empresas de VASCO Group.
- Acciones u omisiones que puedan constituir una infracción del programa para la prevención de la comisión de delitos y Código Ético de VASCO Group.
- Operaciones sospechosas conforme a la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Cualesquiera otras comunicaciones que hagan referencia a infracciones normativas de cualquier otro ámbito, ya sean laborales, civiles, penales o administrativas, que afecten a las sociedades de VASCO Group.

Estas comunicaciones se orientan a hechos que puedan afectar al interés general y que se encuentren dentro del ámbito material de aplicación de la Ley 2/2023, y no deben confundirse con quejas laborales, que son de carácter personal o individual.

Cuando una comunicación se remita por canales distintos de los establecidos o se dirija a personal no responsable de su gestión, se informará al remitente de dicha circunstancia y de que el uso indebido del sistema puede constituir una infracción muy grave. Asimismo, la persona que reciba la comunicación estará obligada a remitirla de forma inmediata al Responsable del Sistema Interno de Información del Grupo, garantizando en todo caso la confidencialidad y protección de la persona informante.

Cada comunicación será tramitada respetando la autonomía de la sociedad implicada, de modo que la gestión del caso, la adopción de medidas y la asunción de responsabilidades correspondan a la empresa afectada.

4. Sujetos habilitados para comunicar

Podrán utilizar el Sistema Interno de Información todas las personas vinculadas a cualquier sociedad de VASCO Group adherida al Sistema, así como determinados grupos de interés externos.

Se consideran personas vinculadas a VASCO Group: integrantes del Consejo de Administración, directivos y directivas, personal trabajador, y cualquier otra persona bajo subordinación jerárquica de las anteriores en cada sociedad, incluidos voluntarios/as, becarios/as y personas trabajadoras en periodos de formación con independencia de que perciban o no una remuneración, así como personas cuya relación todavía no haya comenzado en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de provisión del puesto de trabajo.

Los grupos de interés externos incluyen, entre otros, a los colectivos previstos en la Directiva (UE) 2019/1937 y en la Ley 2/2023, tales como personas trabajadoras autónomas, contratistas, subcontratistas, proveedores y el personal a su servicio.

Aunque el Sistema Interno de Información sea común para todo el Grupo, cada comunicación será gestionada teniendo en cuenta la sociedad específica afectada, garantizando trazabilidad, independencia y responsabilidad individual de cada empresa dentro del Grupo.

5. Vinculación con otras políticas corporativas

El Sistema Interno de Información se integra en el marco general de cumplimiento y gobernanza del Grupo, manteniendo coherencia con el resto de políticas corporativas, en particular el Código Ético y las políticas de cumplimiento normativo aplicables.

Las informaciones recibidas a través del Sistema podrán dar lugar a la aplicación de las medidas previstas en dichas políticas, correspondiendo a cada sociedad la adopción de las actuaciones que procedan en su ámbito de responsabilidad.

La actualización de las políticas corporativas deberá tener en cuenta su posible impacto en el funcionamiento del Sistema Interno de Información de VASCO Group, garantizando en todo caso el mantenimiento de sus principios de confidencialidad, independencia y eficacia.

6. Principios rectores del Sistema Interno de Información

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

- Confidencialidad: Se garantiza la privacidad de la persona informante, la persona denunciada y de todos los terceros implicados, independientemente de la

sociedad afectada. La información solo será compartida con personal autorizado y dentro de los límites necesarios para la investigación.

- Independencia e imparcialidad: El Responsable del Sistema Interno de Información, instructor/a y personas investigadoras deben actuar sin conflictos de interés y con autonomía respecto a cada sociedad. Cuando una comunicación afecte a una sociedad específica, los órganos internos de esa sociedad gestionarán las medidas pertinentes, asegurando imparcialidad y consistencia con las políticas corporativas.
- Protección frente a represalias: Ninguna persona informante de buena fe sufrirá medidas adversas por el simple hecho de comunicar irregularidades. Cada sociedad deberá garantizar la protección de su personal y de los terceros vinculados a su actividad, manteniendo la seguridad y anonimato según corresponda.
- Presunción de inocencia: La persona denunciada será considerada inocente hasta que los hechos se confirmen mediante la investigación correspondiente.
- Transparencia limitada: Se proporcionará información suficiente a las personas afectadas por la investigación, sin comprometer la confidencialidad del proceso ni la seguridad de las personas involucradas. La transparencia se ajustará a la normativa vigente y a las políticas de cada sociedad, manteniendo coherencia a nivel del Grupo.
- Responsabilidad individual de cada sociedad: Cada empresa es responsable de la gestión y resolución de las comunicaciones que le correspondan, garantizando que las medidas correctivas y preventivas sean aplicadas de forma adecuada, sin afectar la independencia operativa de otras sociedades.

7. Gestión de los datos y protección de la información

El Sistema Interno de Información del Grupo VASCO recopila, gestiona y protege los datos conforme a la normativa aplicable, incluyendo el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD). Aunque el Sistema Interno de Información es un sistema común, cada sociedad es responsable de garantizar la legalidad y la protección de los datos de las comunicaciones que le afecten directamente. La gestión de datos se realizará de manera independiente por cada sociedad en coordinación con el Responsable del Sistema Interno de Información del Grupo.

Cualquier dato que resulte irrelevante, innecesario o recogido por error será eliminado de forma inmediata, asegurando que la información tratada sea siempre pertinente y proporcional al objeto de la investigación.

Los datos personales tratados en el Sistema se conservarán únicamente durante el tiempo imprescindible para el cumplimiento de los fines legales. En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema de forma anonimizada. Si se inicia una investigación, los datos podrán tratarse fuera del sistema

de información según la normativa aplicable, procediendo al bloqueo de los mismos conforme al artículo 32 de la LOPDGDD cuando termine la investigación.

Se implementarán medidas técnicas y organizativas que garanticen la integridad, disponibilidad y confidencialidad de los datos. La protección de datos se adaptará a los requisitos legales específicos, asegurando el cumplimiento de la legislación nacional y de las directrices del Grupo.

8. Modalidades disponibles para informar

El Sistema Interno de Información del Grupo está diseñado para garantizar un acceso fácil, seguro, confidencial y, cuando se desee, anónimo. Todas las sociedades del Grupo utilizan el mismo Sistema Interno de Información, asegurando uniformidad en la gestión de las comunicaciones, pero cada sociedad conserva la responsabilidad sobre las denuncias que le afecten directamente.

Las comunicaciones se pueden realizar a través de los siguientes canales internos:

Correo electrónico

- Dirección: canaldedenuncias@vascologistics.com
- Exclusivamente gestionado por el Responsable del Sistema Interno de Información del Grupo.
- Disponible las 24 horas.
- Permite presentar la comunicación de forma detallada y adjuntar documentación.

Plataforma digital / Formulario en línea

- Acceso a través de una dirección web específica del Canal Interno de Denuncias dispuesto por cada sociedad.
- Posibilidad de realizar la comunicación de forma identificada o anónima.
- Plataforma cifrada y conforme al RGPD y la LOPDGDD.
- Permite adjuntar archivos y realizar el seguimiento del estado de la denuncia.

Denuncia verbal o presencial

- La persona informante puede solicitar una reunión directa con el Responsable del Sistema Interno de Información del Grupo mediante correo electrónico o a través del Canal Interno de Denuncias facilitada en página web por cada sociedad.
- La reunión se realizará, en todo caso, dentro de un plazo máximo de siete días desde la solicitud.
- También es posible comunicar la información por vía telefónica al número +34 600901240.
- La comunicación se documentará mediante grabación (previo consentimiento) o acta escrita. La persona informante tendrá la oportunidad de revisar, rectificar y aprobar mediante firma la transcripción de la conversación.

El Sistema Interno de Información del Grupo está preparado para recibir comunicaciones en cualquier formato, escrito o verbal, siempre que la información sea

comprensible y permita llevar a cabo una investigación eficaz, garantizando en todo momento la confidencialidad y protección de la persona informante.

Cada sociedad actuará de manera independiente respecto de las denuncias que le correspondan, manteniendo la coherencia con la estrategia global del Grupo.

9. Recepción y gestión de las comunicaciones

Todas las comunicaciones realizadas a través del Sistema Interno de Información serán recepcionadas por el Responsable del Sistema Interno de Información del Grupo, quien asumirá su gestión, tramitación y supervisión del expediente, pudiendo apoyarse en las áreas o funciones que resulten competentes para la adecuada investigación de las denuncias recibidas.

Si bien el Sistema Interno de Información es único y centralizado para todo el Grupo, cada sociedad mantiene la responsabilidad sobre las comunicaciones que le correspondan directamente. La investigación y las decisiones correspondientes serán asumidas por la sociedad afectada, en coordinación con el Responsable del Sistema Interno de Información del Grupo para garantizar coherencia, seguimiento global y cumplimiento de los estándares de protección y confidencialidad conforme a la normativa aplicable.

El Responsable del Sistema Interno de Información compatibilizará las funciones propias de su puesto o cargo con las correspondientes al sistema, adoptando las medidas necesarias para prevenir y evitar conflictos de interés, garantizando en todo momento imparcialidad, confidencialidad y trazabilidad de las actuaciones.

10. Conflictos de interés

En caso de conflicto de interés, y en particular cuando la persona designada como Responsable del Sistema Interno de Información del Grupo sea objeto de la comunicación o mantenga cualquier vínculo que pueda comprometer su imparcialidad, deberá abstenerse de intervenir en la gestión, tramitación y supervisión del expediente.

Asimismo, se considerará que existe conflicto de interés cuando concurran circunstancias que puedan afectar a la imparcialidad de la investigación dentro de la sociedad afectada, debiendo adoptarse las medidas necesarias para garantizar la independencia del proceso.

En estos casos, la tramitación será asumida por un instructor/a o equipo independiente, designado al efecto, que podrá estar integrado por personal interno no implicado o por profesionales externos especializados, garantizando en todo momento su independencia e imparcialidad.

La persona informante recibirá el correspondiente acuse de recibo y seguimiento del expediente sin intervención de la persona afectada por el conflicto, asegurando la confidencialidad de su identidad y la protección frente a represalias.

Todas las actuaciones serán documentadas, registradas y trazables, en cumplimiento de la Ley 2/2023 y de la normativa vigente en materia de protección de datos.

11. Funciones y obligaciones del Responsable del Sistema Interno de Información

Al Responsable del Sistema Interno de Información de VASCO Group le corresponde garantizar que el Sistema Interno de Información esté diseñado, implantado y gestionado de manera segura y efectiva, de forma que todas las comunicaciones puedan ser recibidas, tramitadas e investigadas dentro de cada sociedad conforme a la normativa aplicable.

El Responsable ejerce sus funciones respecto del conjunto del Grupo, sin perjuicio de que cada sociedad mantenga la responsabilidad sobre las decisiones y actuaciones derivadas de las comunicaciones que le afecten directamente.

Sus principales funciones incluyen:

- Gestión integral del sistema: recepción, registro, clasificación, tramitación y seguimiento diligente de todas las comunicaciones recibidas a través del Sistema Interno de Información del Grupo, garantizando su adecuada asignación a la sociedad afectada.
- Coordinación de la investigación interna: impulso, coordinación y supervisión de las investigaciones, asegurando su correcta realización. La ejecución de las actuaciones y la adopción de medidas corresponderán, en su caso, a la sociedad afectada, respetando su autonomía.
- Confidencialidad y protección: garantizar en todo momento la confidencialidad de la identidad de la persona informante, de las personas mencionadas y de las actuaciones desarrolladas, así como la protección frente a represalias.
- Seguridad del sistema: velar por la integridad, disponibilidad y confidencialidad de la información, asegurando el cumplimiento de la normativa de protección de datos y de seguridad de la información en todas las sociedades del Grupo.
- Independencia y autonomía: ejercer sus funciones sin recibir instrucciones de terceros, con plena autonomía operativa, garantizando la imparcialidad en la gestión del sistema.
- Coordinación entre sociedades: asegurar la coherencia en la aplicación del Sistema Interno de Información en todas las sociedades del Grupo, promoviendo criterios homogéneos de actuación, sin interferir en la responsabilidad individual de cada entidad.
- Medios y recursos: disponer de los medios personales, materiales y tecnológicos necesarios para el adecuado desempeño de sus funciones.

El Responsable del Sistema Interno de Información deberá actuar en todo momento con diligencia, objetividad e independencia, respetando la normativa vigente, en particular la Ley 2/2023 y la legislación en materia de protección de datos, y garantizando el correcto funcionamiento del sistema en el conjunto del Grupo.

12. Criterios para la presentación de las comunicaciones

Las comunicaciones realizadas a través del Sistema Interno de Información de VASCO Group deberán ajustarse a los siguientes criterios, con el fin de garantizar un uso adecuado, eficaz y conforme a la normativa aplicable.

1. Veracidad y buena fe.

Todas las comunicaciones deben ser veraces, deben realizarse de buena fe y deben estar fundadas en la existencia de indicios racionales de la comisión de un acto ilícito, delictivo y/o contrario al Derecho de la Unión Europea, incumplimientos del Código Ético e infracciones penales y administrativas graves o muy graves.

No se exige a la persona informante la certeza absoluta de los hechos comunicados, sino que estos se formulen con una creencia razonable en su veracidad.

2. Soporte de la comunicación

Se recomienda que las denuncias se acompañen de pruebas documentales siempre que sea posible. También son admisibles pruebas testificales, incluido el testimonio de la persona informante, así como instrumentos de reproducción de palabras, imágenes o sonidos.

La comunicación debe incluir, siempre que se conozca, una descripción de la irregularidad o infracción denunciada, la identificación de las personas responsables si son conocidas y la aportación, siempre que sea posible, de documentos o evidencias que respalden la denuncia.

La ausencia de pruebas no impedirá la admisión de la comunicación si existen indicios suficientes para su análisis.

3. Denuncias falsas o de mala fe

El Sistema Interno de Información no podrá utilizarse para fines distintos de los previstos en este reglamento.

La formulación de comunicaciones deliberadamente falsas o realizadas de mala fe podrá dar lugar a la adopción de medidas disciplinarias o legales, sin perjuicio de las responsabilidades que pudieran derivarse conforme a la normativa aplicable. En particular, dichas conductas podrían constituir ilícitos penales, como los delitos de calumnias o injurias previstos en la legislación vigente.

4. Nulidad de restricciones

Cualquier cláusula o disposición contractual que impida o pretenda limitar el derecho a informar a través de este Sistema, incluyendo cláusulas de confidencialidad o renuncias expresas, se considerará nula de pleno derecho y no tendrá efecto alguno frente a las comunicaciones realizadas de buena fe bajo este Reglamento.

5. Finalidad del Sistema

El Sistema Interno de Información tiene como finalidad constituir un mecanismo fiable, seguro y eficaz para la detección y gestión de irregularidades, contribuyendo al cumplimiento normativo y al fortalecimiento de una cultura de integridad en todas las sociedades del Grupo.

Su utilización responsable resulta esencial para garantizar un entorno profesional basado en el respeto a la legalidad, la ética y la responsabilidad compartida.

13. Protección frente a represalias

Aunque el Sistema Interno de Información sea común para todo el Grupo, cada sociedad será responsable de garantizar de manera efectiva la protección frente a represalias dentro de su propio ámbito organizativo y funcional. Esta protección resulta aplicable tanto a personas empleadas y directivos/as, como a terceros vinculados, incluyendo contratistas, proveedores y subcontratistas.

La protección frente a represalias cubre, entre otros:

- Medidas laborales negativas: despido, suspensión, degradación, cambio de funciones o cualquier afectación a la carrera profesional.
- Perjuicios económicos o contractuales: reducción de salarios, beneficios, contratos o pagos asociados.
- Trato desfavorable: marginación, hostigamiento, acoso, intimidación o cualquier conducta que afecte la dignidad de la persona.
- Perjuicios indirectos: amenazas a familiares, colaboradores o representantes legales de la persona informante.

Para garantizar esta protección, VASCO Group y cada una de las sociedades se comprometen a:

- Adoptar medidas preventivas y correctivas inmediatas si se detectan intentos de represalia.
- Garantizar que las decisiones laborales, profesionales o contractuales adoptadas sean objetivas, justificadas y ajenas a la comunicación realizada.
- Supervisar, a través del Responsable del Sistema Interno de Información, que se respeten los estándares de protección.
- Asegurar que cualquier actuación relacionada con la investigación respete la confidencialidad de la identidad de la persona informante y de las demás personas implicadas.

Si la persona informante considera que ha sido objeto de represalias puede comunicarlo de inmediato al Responsable del Sistema Interno de Información del Grupo. La comunicación será investigada de manera diligente, garantizando la independencia, imparcialidad y confidencialidad del proceso.

La sociedad en cuyo ámbito se haya producido la posible represalia será responsable de adoptar las medidas correctivas oportunas, sin perjuicio de la supervisión del Responsable del Sistema Interno de Información del Grupo. Se podrán adoptar medidas disciplinarias contra las personas responsables de las represalias, así como acciones destinadas a la reparación del perjuicio causado.

Así mismo, las personas que actúen como representantes o asesores de la persona informante, así como aquellas que estén vinculadas a ella y puedan verse afectadas, estarán igualmente protegidas frente a cualquier forma de represalia derivada del ejercicio de sus funciones de apoyo.

Se garantizará la adecuada difusión de esta política de protección frente a represalias. Asimismo, se promoverán acciones de formación y sensibilización dirigidas a personas empleadas, directivos/as y terceros vinculados, con el fin de asegurar el conocimiento de la prohibición de represalias, los derechos de las personas informantes y las obligaciones de todas las personas que intervienen en el Sistema Interno de Información.

14. Medidas cautelares

Las medidas cautelares son actuaciones de carácter provisional que cada sociedad podrá adoptar en el marco de la tramitación de las comunicaciones recibidas a través del Sistema Interno de Información, con la finalidad de garantizar el adecuado desarrollo de la investigación, evitar la continuidad de la conducta denunciada y proteger tanto a la persona informante como a las personas implicadas y a la propia organización. Estas medidas carecen de carácter sancionador y se aplicarán conforme a los principios de legalidad, proporcionalidad, necesidad, idoneidad y presunción de inocencia, procurando en todo momento minimizar cualquier perjuicio para las personas afectadas.

La adopción de medidas cautelares procederá cuando existan indicios razonables de la veracidad de los hechos comunicados y concurran circunstancias que justifiquen su implementación, tales como el riesgo de destrucción u ocultación de pruebas, la posible reiteración de la conducta o la necesidad de proteger a la persona informante frente a represalias. Entre otras, podrán consistir en la limitación o suspensión temporal de funciones, la restricción de acceso a sistemas, instalaciones o documentación, la reasignación provisional de puesto o funciones, la suspensión temporal de la relación laboral conforme a la normativa aplicable, o cualquier otra actuación que resulte adecuada y proporcionada a la naturaleza de los hechos.

El Responsable del Sistema Interno de Información podrá proponer la adopción de medidas cautelares cuando resulte necesario para garantizar la adecuada tramitación de la investigación o evitar la continuidad de la conducta, correspondiendo su adopción al órgano competente de la sociedad afectada. Tendrán carácter temporal y se

mantendrán únicamente durante el tiempo imprescindible, siendo objeto de revisión periódica y pudiendo ser modificadas o dejadas sin efecto en función de la evolución de la investigación. En todo caso, se garantizará el respeto a los derechos fundamentales de las personas afectadas, así como la confidencialidad de la información y el adecuado registro de todas las actuaciones realizadas.

15. Procedimiento para la presentación de una comunicación y su gestión

El Sistema Interno de Información del VASCO Group establece un procedimiento común para la gestión de las comunicaciones, garantizando un tratamiento homogéneo en todo el Grupo. No obstante, cada sociedad será responsable de la gestión, investigación y resolución de las comunicaciones que le afecten directamente, bajo la coordinación y supervisión del Responsable del Sistema Interno de Información del Grupo.

1. Formalización y presentación de la comunicación.

El procedimiento se iniciará con la presentación de una comunicación por la persona informante a través de cualquiera de los medios habilitados por el sistema (correo electrónico, plataforma web, verbal o presencial), garantizando confidencialidad y seguridad y, en su caso, anonimato.

La persona informante deberá, en la medida de lo posible, indicar:

- Datos identificativos (opcional si desea permanecer anónima).
- Datos de la persona denunciada.
- Descripción de los hechos denunciados.
- Fecha y hora, o periodo en que ocurrieron los hechos.
- Identificación de testigos, si los hubiera.

2. Recepción de la comunicación y registro.

Todas las comunicaciones serán recepcionadas por el Responsable del Sistema Interno de Información del Grupo y recibirán un código único de identificación para su seguimiento. El código de identificación asociado a la comunicación servirá a la persona informante para realizar un seguimiento del trámite correspondiente y, en su caso, para recibir comunicaciones o aportar nueva información.

Todas las comunicaciones serán registradas en el Registro del Sistema Interno de Información del Grupo. Se trata de un registró único que permitirá la identificación de la sociedad afectada en cada caso, garantizando la trazabilidad, confidencialidad y gestión individualizada de cada comunicación conforme a las responsabilidades de la empresa correspondiente.

3. Acuse de recibo

La persona informante recibirá un acuse de recibo en un plazo máximo de siete días naturales por la misma vía por la que se presentó la comunicación, salvo que ello pueda poner en peligro la confidencialidad de la comunicación. Si la comunicación presenta defectos formales, se podrá solicitar su subsanación.

La persona será informada de sus derechos (confidencialidad y protección frente a represalias).

4. Análisis preliminar

En esta fase inicial, el Responsable del Sistema Interno de Información evaluará la admisibilidad de la comunicación si los hechos entran dentro del ámbito del canal interno. Se valorará, la competencia, la verosimilitud de la información presentada y la suficiencia de las evidencias aportadas. En los casos en que la comunicación aportada presente alguna carencia de información, se podrá solicitar más información a la persona informante.

Analizada la comunicación, el Responsable del Sistema Interno de Información adoptará una decisión inicial: apertura de la investigación porque hay indicios razonables o archivo motivado cuando la denuncia resulte manifiestamente infundada, dejando constancia de los motivos.

En el caso de inadmisión, el Responsable del Sistema Interno de Información notificará la decisión de inadmisión de manera motivada a la persona informante salvo que la comunicación fuera anónima o el informante hubiera renunciado a recibir comunicaciones. La inadmisión supondrá la finalización del procedimiento.

En caso de admisión y apertura de expediente, la decisión de admisión a trámite de la comunicación se comunicará a la persona informante, excepto cuando la información sea anónima o cuando el informante haya renunciado a recibir comunicaciones. Con la admisión se iniciará la fase de instrucción del procedimiento.

Cuando los hechos pudieran ser indiciariamente constitutivos de delito, la comunicación será remitida al Ministerio Fiscal. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

Desde la decisión de admisión, se dará conocimiento a la persona afectada de la existencia de las actuaciones y de los hechos relatados, así como de sus derechos. En ningún caso a la persona afectada se le revelarán datos que pudieran identificar a la persona informante, ni se le dará acceso a la comunicación. También se advertirá a la persona afectada de las consecuencias de revelar información a terceros en los términos previstos en la Ley 2/2023.

Todas las comunicaciones que se realizan con la persona afectada quedarán documentadas en el sistema dejando constancia de su resultado, tanto si han sido recogidas expidiéndose el correspondiente acuse de recibo, como si han sido rehusadas.

4. Investigación interna.

En el ámbito de cada sociedad, la investigación de las comunicaciones será llevada a cabo por un instructor/a o, en su caso, por un equipo investigador designado al efecto. La designación se realizará atendiendo a la naturaleza de los hechos, garantizando en todo momento la independencia, imparcialidad y cualificación de las personas encargadas de la investigación, sin interferir en la actuación de la autoridad competente si se diera el caso.

El instructor/a o equipo investigador podrá estar integrado por personal interno de la sociedad, siempre que no exista conflicto de interés, o por profesionales externos especializados cuando la complejidad, sensibilidad o circunstancias del caso así lo requieran. En ningún caso podrán participar en la investigación personas que mantengan relación directa o indirecta con los hechos objeto de la comunicación o con las personas afectadas que pueda comprometer su objetividad.

La sociedad afectada será responsable de la ejecución de la investigación, sin perjuicio de la coordinación y supervisión del Responsable del Sistema Interno de Información del Grupo.

Las actuaciones en la investigación podrán incluir:

- Recopilación y análisis de documentación.
- Entrevistas con personas denunciadas, testigos o terceros.
- Recopilación de cualquier otra evidencia relevante.

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. Se considerarán lícitos los tratamientos de datos personales necesarios para la aplicación de la ley.

Toda la documentación (informes, pruebas, actas, decisiones) se almacenará bajo la supervisión del Responsable del Sistema Interno de Información, de forma que se asegure la confidencialidad y se garantice la trazabilidad de todas las acciones sobre el expediente.

Se podrán adoptar medidas cautelares cuando existan indicios razonables de la veracidad de los hechos comunicados y concurran circunstancias que justifiquen su implementación, tales como el riesgo de destrucción u ocultación de pruebas, la posible reiteración de la conducta o la necesidad de proteger a la persona informante frente a represalias.

Como resultado de la investigación realizada, el instructor/a o equipo investigador elaborará un informe que incluirá los hechos probados, las evidencias, las conclusiones y recomendaciones.

5. Resolución del expediente.

Finalizada la investigación interna, la dirección o comité competente de la sociedad afectada adoptará la decisión que corresponda y se procede a la resolución del expediente, que puede dar lugar como resultado:

- Al archivo de la denuncia
- A la adopción de medidas disciplinarias o correctivas
- A la comunicación a las autoridades competentes
- A cambios en procesos internos

Si de la investigación resultasen confirmados los hechos denunciados, en primer lugar, la sociedad adoptará con carácter inmediato todas las medidas que sean necesarias para poner fin a tales actos o para evitar que ocurran. Posteriormente, en función de la gravedad de los hechos, se podrán iniciar las acciones legales que correspondan contra la persona o personas presuntamente responsables de los mismos, incluyendo las consecuencias disciplinarias internas y cuantas otras se estimen pertinentes.

La información que contendrá el expediente es el siguiente:

- Identificación del número de expediente, de la persona informante, de la persona denunciada y del instructor del procedimiento o equipo investigador.
- Información y documentación aportada en la denuncia y recabada en la investigación.
- Resumen de los hechos denunciados y de la investigación llevada a cabo.
- Decisión adoptada y medidas a implementar.

Además, se notificará a la persona informante (en la medida en que este identificada y no haya hecho uso de su renuncia de comunicarse con el Responsable del Sistema) y a la persona afectada, al menos:

a) Una exposición de los hechos relatados junto con el número de expediente, la fecha de registro y la del acuerdo de admisión.
b) Las actuaciones realizadas con el fin de comprobar la verosimilitud de los hechos que recogerá, al menos y de manera sucinta, las alegaciones formuladas por la persona afectada, incluida la entrevista en su caso y la documentación aportada por éste o recabada por el Responsable del Sistema a través de terceros y cuantas otras informaciones en las que se base la resolución adoptada.
c) Las conclusiones alcanzadas en la instrucción y la valoración de las diligencias y de los indicios que las sustentan.
d) Las decisiones adoptadas.

El plazo para la tramitación del expediente y adopción de una decisión al respecto no podrá exceder los tres meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante, a partir del vencimiento del plazo de siete días después de efectuarse la comunicación, 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.

6. Conservación de la información.

Una vez finalizado el proceso, toda la documentación relacionada con las comunicaciones recibidas será conservada durante el tiempo necesario para cumplir con la normativa aplicable, incluyendo la legislación en materia de protección de datos y lo establecido en la Ley 2/2023, asegurando su integridad, confidencialidad y trazabilidad.

Cada sociedad del Grupo será responsable de garantizar la correcta conservación, confidencialidad, seguridad y trazabilidad de la información correspondiente a los expedientes tramitados en su ámbito, de conformidad con la normativa aplicable, sin perjuicio de las funciones de coordinación, supervisión y verificación del cumplimiento de estándares que corresponden al Responsable del Sistema Interno de Información del Grupo.

16. Obligaciones de las personas que tomen parte en la investigación

Todas las personas que intervengan en la investigación de una comunicación recibida a través del Sistema Interno de Información del Grupo deberán cumplir con las siguientes obligaciones:

- Deber de colaboración: Participar activamente en la investigación, aportando la información, documentos o evidencias que se requieran en el marco de la investigación; y, facilitar el acceso a sistemas, archivos o áreas bajo su responsabilidad, dentro de los límites legales y organizativos.
- Deber de diligencia y veracidad: Responder de manera completa, objetiva y veraz a todas las solicitudes de información o aclaración relacionadas con la investigación; actuar con profesionalidad, imparcialidad y respeto a los principios de buena fe y transparencia; y, abstenerse de emitir juicios o valoraciones personales que puedan afectar la imparcialidad de la investigación.
- Deber de confidencialidad: Mantener en estricta confidencialidad toda información, datos, documentos y actuaciones a los que tengan acceso durante la investigación, incluyendo la identidad de la persona informante, de las personas denunciadas y de terceros implicados; y, abstenerse de utilizar la información obtenida para fines distintos a los de la investigación.
- Independencia y neutralidad: Actuar de forma independiente, evitando cualquier conflicto de interés o influencia externa que pueda comprometer la imparcialidad de la investigación; y, en caso de conflicto de interés, la persona deberá abstenerse de intervenir, y se activará el procedimiento para designar un instructor interno alternativo o, si fuera necesario, un profesional externo.

El incumplimiento de estas obligaciones podrá dar lugar medidas disciplinarias internas proporcionales a la gravedad de la infracción; responsabilidades legales, en caso de vulneración de la normativa aplicable (Ley 2/2023, RGPD, legislación laboral o penal); y, evaluación y adopción de medidas correctivas para proteger la integridad del Sistema Interno de Información y la seguridad de las personas afectadas.

La investigación de las comunicaciones recibidas a través del Sistema Interno de Información del Grupo se regirá por los principios de confidencialidad, imparcialidad, protección, diligencia y respeto a los derechos de las personas implicadas.

De esta manera, se asegura que cada sociedad mantiene su autonomía y responsabilidad legal, mientras que el Sistema Interno de Información del Grupo se

aplica de forma coherente, uniforme y justa, garantizando siempre la protección de las personas implicadas, la confidencialidad de la información y el cumplimiento de la normativa vigente.

17. Sanciones y medidas derivadas de un incumplimiento

Las medidas a adoptar dependerán de la gravedad y naturaleza del incumplimiento, así como del impacto sobre la empresa afectada y el Grupo en su conjunto. Todas las acciones se aplicarán garantizando la proporcionalidad, la confidencialidad y la trazabilidad de las decisiones.

1. Medidas disciplinarias internas

   Para incumplimientos leves o internos, que no supongan riesgos legales significativos ni afecten a otras sociedades del Grupo, se aplicarán medidas disciplinarias, tales como advertencias, amonestaciones o cualquier otra sanción prevista en la normativa interna de la sociedad correspondiente.

2. Resolución de relaciones laborales o contractuales

   Cuando los hechos lo justifiquen y conforme a la legislación aplicable, se podrán adoptar medidas que afecten a la relación contractual, incluyendo la suspensión temporal o la resolución del contrato de trabajo o de servicios, siempre respetando los derechos de las personas involucradas y la presunción de inocencia.

3. Actuaciones legales y comunicación a autoridades competentes

   En los casos en que la investigación identifique posibles ilícitos penales, administrativos o incumplimientos graves de normativa aplicable, la sociedad afectada remitirá la información a las autoridades competentes, coordinando la actuación con los órganos del Grupo si se detecta impacto transversal en otras sociedades.

Independientemente de las medidas disciplinarias o legales, se evaluará la necesidad de revisar, modificar o reforzar la normativa interna, los procedimientos operativos y los controles existentes, con el objetivo de prevenir la repetición de incumplimientos, consolidar una cultura de cumplimiento y asegurar la integridad de las sociedades del Grupo.

Todas las medidas adoptadas quedarán registradas en el expediente correspondiente, de manera confidencial y segura. Solo las personas con responsabilidad directa en el seguimiento del Sistema Interno de Información y, en su caso, autoridades competentes, tendrán acceso a esta información, respetando siempre la normativa de protección de datos y la Ley 2/2023.

18. Derechos y deberes de las personas informantes y denunciadas

El Sistema Interno de Información protege tanto a las personas que presentan comunicaciones como a las que son objeto de las mismas, garantizando un equilibrio entre confidencialidad, protección y derecho a la defensa. Cada sociedad mantiene la responsabilidad de aplicar estas garantías dentro de su ámbito, mientras se asegura la uniformidad de criterios a nivel de Grupo.

Personas informantes

Todas las comunicaciones realizadas a través del Sistema Interno de Información se gestionarán de manera confidencial, y la identidad de la persona informante solo podrá ser revelada:

- Con su consentimiento expreso, o
- A la autoridad competente para la investigación de los hechos, cuando la ley así lo requiera.

Se garantiza que la persona informante de buena fe no sufrirá represalias, discriminación ni perjuicio alguno por haber presentado la denuncia. Esta protección se extiende también a los representantes legales o asesores que actúen en funciones de apoyo a la persona informante.

Derechos de las personas informantes:

- Acceder al Sistema y conocer su existencia.
- Mantener la confidencialidad y, en su caso, anonimato.
- Ser protegida en materia de datos personales.
- No ser objeto de represalias.
- Ser informada sobre la resolución o archivo de la denuncia.

Deberes de las personas informantes:

- Actuar con buena fe, evitando comunicaciones falsas o maliciosas.
- Proporcionar información veraz y, en la medida de lo posible, documentada sobre los hechos denunciados.
- Mantener confidencialidad sobre el contenido de la investigación.

Personas denunciadas

La persona afectada será informada de la existencia de la comunicación y de los hechos que se le atribuyen en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación. Bajo ninguna circunstancia se le facilitará acceso a la identidad de la persona informante ni a datos que permitan su identificación.

Derechos de las personas denunciadas:

- Ser informada sobre la existencia de la investigación y recibir un resumen de la denuncia.
- Acceder a los datos registrados, con las excepciones legales correspondientes (identidad de la persona informante y terceros).
- Ser informada sobre la resolución o archivo de la denuncia.
- Ser tratada con presunción de inocencia, dignidad y respeto, sin estigmatización ni prejuicio.

Deberes de las personas denunciadas:

- Colaborar con la investigación proporcionando información veraz, completa y objetiva cuando se le requiera.
- Mantener la confidencialidad sobre los datos y actuaciones del procedimiento.

Cada sociedad es responsable de garantizar que los derechos y deberes señalados se respeten dentro de su organización, asegurando la coherencia con el Sistema Interno de Información y facilitando la coordinación cuando la investigación implique hechos que puedan afectar a varias sociedades. La supervisión y el seguimiento de estas garantías serán realizados por el Responsable del Sistema Interno de Información, con apoyo de instructores internos alternativos o externos, según corresponda.

19. Canales externos al sistema interno de información

El Sistema Interno de Información de VASCO Group constituye el canal preferente para la comunicación de infracciones y conductas irregulares. Sin embargo, las personas informantes pueden optar por utilizar canales externos cuando consideren que existe riesgo de represalias, dudas sobre la confidencialidad del procedimiento, o que la comunicación no será gestionada de manera adecuada a través del Sistema Interno de Información.

Se ruega que no se usen ambos de forma concurrente, pues se duplicaría el trabajo y se podrían producir inconsistencias entre las decisiones de ambos tipos de canales.

A nivel estatal, este canal está gestionado por la Autoridad Independiente de Protección del Informante (AIPI), una autoridad administrativa independiente, con personalidad jurídica propia y plena capacidad de actuación pública y privada. Entre sus funciones está asegurar que la persona que informa no sufra represalias, adoptar medidas de protección (cautelares o de apoyo) y coordinarse con otras instituciones si es necesario.

Además, junto a la Autoridad estatal, existen autoridades autonómicas a las que se han atribuido competencias para actuar como canales externos en su ámbito territorial, como es el caso de Andalucia, Cataluña, Comunidad Valenciana y Galicia. Estos canales son gestionados por organismos públicos competentes en la respectiva comunidad autónoma, con plena independencia en el tratamiento de la información recibida. La normativa propia de cada comunidad autónoma determina de forma específica cuales son las categorías de infracciones que, en cada caso, asume su canal externo autonómico.

La utilización de los canales autonómicos no limita la opción de recurrir al canal estatal ni al Sistema Interno de Información de VASCO Group. La persona informante puede elegir el canal que considere más adecuado según sus circunstancias y nivel de confianza.

20. Coordinación con autoridades externas

El Sistema Interno de Información del Grupo contempla la posibilidad de que determinadas comunicaciones sean trasladadas o compartidas con autoridades externas siempre que ello sea necesario para el cumplimiento de la ley, la prevención de delitos o la protección de la integridad de las sociedades.

1. Principios de coordinación:

La coordinación con autoridades externas se realizará bajo los siguientes principios:

- Confidencialidad y protección de la persona informante: en todo momento se garantizará la identidad de la persona informante, salvo que la normativa exija expresamente su revelación.
- Legalidad y proporcionalidad: toda comunicación hacia autoridades externas se realizará respetando estrictamente la normativa aplicable, incluyendo protección de datos, privacidad y seguridad de la información.
- Registro y trazabilidad: todas las comunicaciones remitidas a autoridades externas se documentarán, incluyendo la fecha, el organismo receptor, el contenido remitido y las razones de la remisión, asegurando transparencia y auditoría interna.

2. Autoridades competentes

Dependiendo del ámbito y naturaleza de la denuncia, las comunicaciones podrán remitirse a:

- Autoridades estatales o autonómicas: como los canales externos de denuncias previstos en la Ley 2/2023 o en normativas equivalentes en cada Comunidad Autónoma, por ejemplo Andalucia, Cataluña, Comunidad Valenciana y Galicia.
- Organismos internacionales o jurisdicciones extranjeras: cuando la irregularidad afecte a operaciones transnacionales, se coordinará con autoridades competentes en otros países o con organismos supranacionales, como autoridades de la Unión Europea, Interpol u organismos internacionales de supervisión financiera.
- Órganos reguladores sectoriales: en caso de denuncias que involucren sectores específicos sujetos a supervisión externa, como transporte, logística, comercio internacional o finanzas.

3. Procedimiento de remisión

El Responsable del Sistema Interno de Información realizará un análisis preliminar de las comunicaciones recibidas a fin de determinar si de su contenido se desprenden

indicios de infracción penal o de afectación a los intereses financieros de la Unión Europea, en cuyo caso procederá a su remisión a la autoridad competente. Se asegurará que la remisión preserve la confidencialidad y la seguridad de los datos, limitando la información remitida a lo estrictamente necesario para la investigación.

Se notificará a la persona informante sobre la remisión de la comunicación, salvo que la ley prohíba expresamente tal notificación. Se documentará todo el procedimiento en el Registro de comunicaciones, garantizando trazabilidad, control interno y posibilidad de auditoría.

4. Coordinación con canales externos estatales y autonómicos

El Sistema Interno de Información del Grupo mantiene contacto permanente con los canales externos oficiales, asegurando que las denuncias sean derivadas de manera correcta y conforme a la legislación vigente. La coordinación incluye la verificación de recepción, acuse de recibo y seguimiento, siempre protegiendo la identidad de la persona informante.

Se revisarán periódicamente los protocolos de coordinación para garantizar eficiencia, seguridad y cumplimiento legal.

5. Salvaguardas internacionales

En caso de transferencias de datos hacia jurisdicciones extranjeras, se respetarán las normas de protección de datos internacionales aplicables, incluyendo acuerdos de confidencialidad y mecanismos de transferencia legal (por ejemplo, cláusulas contractuales tipo, decisiones de adecuación o leyes equivalentes).

La coordinación con autoridades internacionales se limita a la información estrictamente necesaria para la investigación y no compromete derechos fundamentales de la persona informante ni de terceros involucrados.

21. Consultas

Cualquier consulta al respecto de lo establecido en este reglamento puede ser enviada a través de canaldedenuncias@vascologistics.com, indicando en el asunto “Consulta”.

22. Entrada en vigor y revisión del reglamento

El presente reglamento ha sido aprobado por los órganos de administración de las sociedades adheridas al Sistema Interno de Información común de VASCO Group. Será de aplicación a todas las sociedades que forman parte del Grupo, respetando la autonomía y responsabilidad individual de cada una.

Además, el reglamento será revisado de manera periódica con el fin de:

- Actualizar y mejorar su contenido.
- Corregir posibles deficiencias o vacíos detectados en su aplicación en alguna sociedad del Grupo.
- Garantizar su adecuación a la normativa vigente.
- Asegurar la eficacia, eficiencia y fiabilidad del Sistema Interno de Información.

La responsabilidad de la revisión corresponde al órgano de gobierno de cada sociedad, contando con la participación del Responsable del Sistema Interno de Información del Grupo y, cuando sea necesario, de asesores externos especializados.

Cualquier modificación o actualización será documentada, comunicada y coordinada con cada sociedad del Grupo, garantizando que su implementación respete la independencia operativa de cada empresa y mantenga los principios de confidencialidad, protección y efectividad del Sistema Interno de Información.

23. Mecanismos de seguimiento y reporte

El Responsable del Sistema Interno de Información del Grupo tiene la obligación de asegurar un seguimiento diligente de todas las comunicaciones recibidas a través del Sistema Interno de Información y de reportar de manera periódica al Consejo de Administración y a los órganos de gobierno competentes de cada sociedad, garantizando transparencia, trazabilidad y mejora continua del sistema, respetando la autonomía y responsabilidad individual de cada sociedad.

1. Contenido de los informes

Los informes periódicos incluirán, entre otros, los siguientes elementos:

- Número y tipo de denuncias recibidas.
- Estado de las investigaciones.
- Medidas adoptadas.
- Evaluación de la eficacia del Sistema Interno de Información.
- Análisis de tendencias y riesgos.

2. Confidencialidad y anonimización

Toda información incluida en los informes será anonimizada, garantizando la protección de la identidad de la persona informante, de la persona denunciada y de terceros implicados. Solo se podrá revelar información personal o identificativa cuando la ley lo exija o en el marco de procedimientos judiciales o administrativos, respetando siempre el principio de necesidad y proporcionalidad.

3. Frecuencia y formato de los informes

Los informes se elaborarán semestralmente, salvo que circunstancias extraordinarias exijan reportes adicionales. Podrán presentarse de manera escrita y/o digital, utilizando formatos estandarizados que faciliten la revisión, seguimiento y auditoría de las actuaciones en todas las sociedades del Grupo.

Los informes internos y la información compartida se anonimizarán, limitando el acceso solo a personal autorizado y evitando la exposición de la identidad de las personas informantes y denunciadas. Cada sociedad puede tener acceso solo a estadísticas agregadas (número de casos, áreas afectadas, tendencias), sin acceso a identidades ni detalles de expedientes que no correspondan.

4. Uso de los informes para la mejora continua

Los informes permitirán:

- Evaluar la eficacia del Sistema Interno de Información del Grupo.
- Identificar áreas de mejora en los procedimientos, controles internos y políticas corporativas.
- Implementar acciones preventivas para reducir riesgos legales, éticos y financieros.
- Asimismo, servirán para la formación continua del personal y la promoción de una cultura de cumplimiento y transparencia dentro de cada sociedad y del Grupo en su conjunto.

5. Trazabilidad y auditoría

Todos los informes, así como la información que los sustenta, quedarán registrados y trazables dentro del sistema, de manera que puedan ser auditados interna o externamente. La trazabilidad garantizará la integridad de los datos, la rendición de cuentas y la comprobación de que las actuaciones se realizaron conforme a la normativa vigente, a las políticas internas y respetando la independencia operativa de cada sociedad.