Política Sistema Interno de Información

Fecha	Revisión	Responsable	Asunto	Cambios significativos
	0	Comité de Compliance	Nueva redacción	

ÍNDICE

1. OBJETIVO

El pasado 13 de marzo entró en vigor 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.

La finalidad última de esta norma reside en garantizar la protección de aquellos ciudadanos que, en un contexto laboral o profesional, informen sobre posibles vulneraciones del ordenamiento jurídico en el marco de dicha relación.

Con ello, y con el objetivo de dar cumplimiento a esta norma, esta política contiene una descripción de los elementos claves, tanto humanos como organizativos, tecnológicos y documentales, que Grupo Freixenet[1] aplicará para proteger la información recibida por los Informantes, así como los datos de carácter personal.

Asimismo, recogerá la creación de un Sistema Interno de Información (en adelante, ``S.I.I.´´), y enunciará los principios generales en materia de defensa del Informante, describiendo su funcionamiento, el canal interno habilitado, los tiempos a cumplir, y la Persona Responsable de dicho sistema.

Así las cosas, como compañía queremos poner en conocimiento a la totalidad de personas que mantengan alguna relación profesional o laboral, de la posibilidad de informar sobre prácticas irregulares que tengan lugar en la propia organización a través del mecanismo establecido en ésta política y que se detallará más adelante, con la finalidad de corregirla o reparar cuanto antes los posibles daños.

La organización pone a disposición de cualquier persona que tenga una relación laboral o profesional un único canal interno, garantizando en todo caso la confidencialidad, así como dando la posibilidad a éstos de informar de forma anónima, si así lo prefieren.

En todos los niveles de Grupo Freixenet, se velará por la aplicación real y efectiva de esta Política de manera que se proteja adecuadamente a los Informantes de posibles represalias que puedan sufrir, así como fortalecer la cultura de información en la compañía.

Grupo Freixenet aplicará un criterio de tolerancia cero respecto a cualquier acto de represalia que pueda sufrir un Informante cuando transmita o ponga conocimiento a través del canal interno previsto en ésta Política de cualquier acto u omisión que pueda constituir una infracción del Derecho de la Unión Europea o infracción penal o administrativa grave o muy grave a los efectos previstos en la norma en cuestión.

[1] Freixenet, S.A.; Segura Viudas, S.A.U., Comercial Grupo Freixenet, S.A.; y Unió Cellers del Noya, S.A. así como cualquier otra sociedad española filial o participada mayoritariamente respecto de la que, de forma directa o indirecta, se ejerza un control efectivo por Freixenet, S.A.

Todos los miembros del Grupo Freixenet deben familiarizarse a fondo con esta política, así como con otras políticas y procedimientos y el Código de Conducta del Grupo Geschwister Oetker.

La presente política es parte de un programa de compliance más amplio y otras políticas y procedimientos pueden recoger áreas más específicas sobre riesgos legales y de compliance u otros requerimientos exigibles según cada país. Los miembros del Grupo Freixenet deberán remitirse a dichas otras políticas y procedimientos para disponer de un mayor conocimiento sobre situaciones concretas y, en caso de tener alguna duda o precisar alguna aclaración, deben contactar con su superior jerárquico (de ser aplicable) o el Comité de Compliance.

Esta política será adaptada a los cambios normativos y regulatorios que se produzcan en el futuro.

2. ÁMBITO DE APLICACIÓN

a. **Ámbito societario**: La presente política se aplica a todas las empresas que conforman el Grupo Freixenet, así como a los Terceros tal y como se indica más adelante.
b. **Ámbito personal**: Esta política es aplicable a todos los niveles de Grupo Freixenet, incluyendo los órganos de administración, cargos directivos, órganos de control, totalidad del personal. Personas que tengan la condición de trabajadores por cuenta ajena de Freixenet, y autónomos, accionistas y personas pertenecientes al órgano de administración, dirección o supervisión de Freixenet, incluidos los miembros no ejecutivos. Cualquier persona que trabaje bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores de Freixenet. También se incluyen a las personas informantes que comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral o estatutaria ya finalizada, personal voluntario, becario, personas trabajadoras en periodos de formación con independencia de que perciban o no una remuneración, así como a aquellos cuya relación todavía no haya comenzado, en los casos en que la información de la infracción haya sido obtenida durante el proceso de selección o de negociación precontractual.
c. **Ámbito relacional**: el ámbito de aplicación de esta política se extenderá a los proveedores, distribuidores y clientes del Grupo Freixenet.
d. **Ámbito geográfico**: Esta política se aplicará a nivel nacional, dando cumplimiento por ello a la legislación española y europea que en su caso aplique.

3. NORMATIVA APLICABLE

Esta política está redactada para dar cumplimiento a la siguiente normativa:

a. Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019.
b. 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.
c. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

4. DEFINICIONES

a). Informante

El término "Informante" significa:

- Cualquier persona que informe sobre vulneraciones del ordenamiento jurídico en el marco de una relación profesional o laboral.
- Cualquier persona que informe sobre vulneraciones del ordenamiento jurídico, aunque hayan finalizado su relación profesional, voluntarios, trabajadores en prácticas o en periodo de formación, personas que participen en procesos de selección, así como las personas que prestan asistencia a los informantes, a las personas de su entorno que puedan sufrir represalias, así como a las personas jurídicas propiedad del informante, entre otras.

b). Vulneración ordenamiento jurídico

Tendrá la consideración de vulneraciones del ordenamiento jurídico y, por tanto, serán cuestiones que se podrán informar a través del canal interno habilitado:

- Acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea[2].
- Acciones u omisiones que puedan ser constitutivas de infracciones penales o administrativas graves o muy graves según lo dispuesto en la normativa mencionada anteriormente.

c). Terceros

El término "Terceros" significa cualquier proveedor, distribuidor, consultor, agente, bróker u otra persona física o jurídica que no forme parte del Grupo Freixenet y que tenga alguna relación profesional con la organización.

[2] Quedan incluidos los siguientes sectores: contratación pública, servicios, productos y mercados financieros, y prevención del blanqueo de capitales y financiación del terrorismo, seguridad de productos y conformidad, seguridad del transporte, protección del medio ambiente y clima, protección frente a las radiaciones y seguridad nuclear, seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales, salud pública, protección de los consumidores, protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información.

d). Represalias

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.

5. SISTEMA INTERNO DE INFORMACIÓN

Como se ha expuesto brevemente en la introducción, por la presente se constata la existencia en la compañía de un Sistema Interno de Información, que permitirá, a través de un único canal interno habilitado, comunicar cualquier tipo de infracción de las mencionadas anteriormente, garantizando la confidencialidad del Informante y de cualquier otra persona mencionado en dicha comunicación, impidiendo en todo caso el acceso de personal no autorizado.

El Órgano de Administración es el responsable de la implementación del S.I.I. y tendrá la condición de Responsable del Tratamiento de los Datos Personales de conformidad con la normativa en materia de protección de datos.

Así las cosas, cabe mencionar que, dado que la plataforma integrada está estructurada dentro del sistema del grupo Henkell Freixenet, Don Thomas Herrmann, actual Compliance Coordinator del grupo Henkell Freixenet, actuará como gestor externo del Sistema Interno de Información, no pudiendo clasificar ni filtrar las informaciones, sino simplemente recibirlas y leerlas. En este caso, el Sr. Herrmann actuará como encargado de protección de datos a efectos de la legislación sobre protección de datos personales, garantizando en todo momento las garantías de respeto de la independencia, confidencialidad y protección de datos.

Para ello, la compañía:

A. Ha integrado todos los canales existentes a día de hoy en un único canal interno que permita presentar comunicaciones tanto verbalmente, dirigiéndose directamente al Responsable del Sistema de Información, como por escrito a través de la plataforma que más adelante se especifica.
B. Ha nombrado a un Responsable del S.I.I.
C. Cuenta con un procedimiento de gestión de información que trata de forma efectiva las comunicaciones recibidas.

5.1. Integración canal interno de información

Hasta el momento, la organización contaba con distintos canales internos de comunicación, según la materia específica de la que se tratara.

1. En primer lugar, en virtud del Protocolo contra el Acoso, la queja o solicitud de apoyo y asistencia se realizaba ante las personas de referencias enumeradas en el anexo adjunto al mismo, tanto de forma verbal como escrita y a través de cualquier medio.

2. En segundo lugar, en materia de protección de datos, cualquier persona podía dirigirse directamente al Data Protection Officer (``DPO´´) a través de la siguiente dirección de correo electrónico gdpr@freixenet.com.

3. En tercer y último lugar, cualquier persona podía denunciar aquella conducta genérica presuntamente irregular, a través de alguna de las siguientes vías:

    a. Acudir inmediatamente al Comité de Compliance;
    b. Contactar con la organización a través del Sistema de Comunicación del Grupo Freixenet:
        - Envío de mensajes anónimos: www.report-securely.eu/henkell-freixenet;
        - Envío de mensajes no anónimos mediante correo electrónico a la organización de Compliance del Grupo Freixenet España: compliance@freixenet.com;
        - Envío de mensajes no anónimos mediante correo electrónico a la organización de Compliance del Grupo Henkell-Freixenet Internacional: compliance@henkell-freixenet.com.

Con la entrada en vigor de dicha norma, los anteriores canales existentes pasan a integrarse en **un único canal**. Se puede acceder a este canal interno de información, el cual permite realizar comunicaciones por escrito (y de forma anónima en caso de ser preferido) a través de la siguiente plataforma: www.report-securely.eu/freixenet

Este único canal permite las comunicaciones entre los Informantes y el Responsable del Sistema, aun siendo las mismas anónimas, con la finalidad de poder recabar toda la información que en su caso sea necesario para iniciar la investigación, pudiendo ser solicitada información adicional a la persona Informante, si así se considera necesario.

Sin perjuicio de lo anterior, a solicitud del Informante, se puede solicitar mantener una reunión presencial. En ese caso, se advertirá al Informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo a lo que establece la normativa en materia de protección de datos vigente.

5.2. Responsable del Sistema Interno de Información

El órgano de administración ha designado a Don Thomas Scholl, actual Chief Financial Officer y miembro del Comité de Compliance del Grupo Freixenet como el Responsable del Sistema Interno de Información sobre quien recaerá la responsabilidad de gestionar dicho sistema. En caso de que el Sr. Scholl se encuentre fuera de la oficina, pasará a ser el Responsable del Sistema Interno Don Josep Palau, actual Chief Technology Officer y miembro del Comité de Compliance.

Sin perjuicio de lo anterior, y según la materia específica de la que trate la comunicación recibida, el Sr. Scholl, y en su ausencia el Sr. Palau, iniciará las investigaciones pertinentes con el gestor que en cada caso resulte necesario siempre garantizando la confidencialidad de los Informantes como de Terceros que aparezcan en las comunicaciones, así como de su contenido.

La estructura del Sistema Interno de Información queda detallada en el **Anexo I** adjunto a la presente política.

5.3. Procedimiento de gestión de informaciones

Este procedimiento de gestión de informaciones persigue el objetivo de clarificar el modo en que cualquier Informante puede informar sobre cualquier acto u omisión y ser conocedor de los plazos y garantías con los que contará:

a) Como se ha especificado en el apartado 5.1., actualmente sólo existe un único canal interno, al cual se puede acceder a través del siguiente hipervínculo: www.report-securely.eu/freixenet En dicha plataforma habrán dos opciones:

   1. En primer lugar, la opción de enviar una comunicación nueva, tanto de forma anónima o con reserva de la identidad, tanto de forma manifiesta, y,
   2. En segundo lugar, la posibilidad de dar seguimiento a una comunicación que se haya realizado de forma anónima.

b) Al hacer la comunicación, y en el caso de que quiera eliminar su anonimato, el Informante podrá indicar su nombre y un correo electrónico a efectos de recibir notificaciones.

c) Asimismo, la plataforma le solicitará que cree una contraseña segura para poder tener acceso al buzón de la información enviada, comprobar el estado de procesamiento, así como comunicarse con el Responsable del Sistema de Información.

d) Siendo la comunicación anónima o no, el Informante podrá dar seguimiento al estado de su comunicación con el ID de referencia y la contraseña individual asignada en el momento que presentó su comunicación. Asimismo, en caso de haber proporcionado una

dirección de correo electrónico, el Informante recibirá en dicha dirección el ID de referencia, así como el acuse de recibo de la comunicación enviada en un plazo máximo de siete (7) días naturales, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.

e) En el caso de que se solicite una reunión presencial, la misma se llevará a cabo dentro del plazo máximo de siete (7) días.

f) La persona afectada tendrá el derecho de ser informada de las acciones u omisiones que se le atribuyen, y a ser oída en cualquier momento. Dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.

g) El Responsable del Sistema, junto con los gestores especificados según la materia que se trate, dará respuesta a las actuaciones de investigación en un plazo máximo de tres (3) meses a contar desde la recepción de 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 (3) meses adicionales.

h) Se remitirá la información al Ministerio Fiscal con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

6. PRINCIPIOS DEL SISTEMA INTERNO DE INFORMACIÓN

La estrategia de la empresa en materia de protección de las personas que informen sobre infracciones normativas cumplirá con los principios de confidencialidad, integridad, autenticidad y trazabilidad de la información, presunción de inocencia y protección de datos personales:

a) Confidencialidad

El principio de confidencialidad garantiza que la información sólo sea accesible para los usuarios autorizados a acceder a ella y que no podrá ser divulgada a terceros sin la correspondiente autorización.

Así las cosas, en todo momento se asegura la extrema confidencialidad en las Informaciones recibidas en tanto será únicamente el Responsable del Sistema, así como los gestores designado según la materia, los que tengan acceso a las comunicaciones recibidas en cuestión.

Asimismo, esta confidencialidad es garantizada aun cuando la Información sea remitida por un canal de denuncias que no sea el establecido y delimitado en la presente política. Por ello, se formará al personal con el objetivo de que sea conocedor de la obligación de trasladar al Responsable del Sistema cualquier Información de ésta índole, así como de la infracción que supone quebrantar dicha confidencialidad.

b) Integridad

El principio de integridad garantiza que la información se mantiene libre de modificaciones y que no ha sido alterada por personas o procesos.

c) Autenticidad y trazabilidad de la información

El principio de autenticidad y trazabilidad de la información garantiza que se llevarán a cabo las investigaciones pertinentes a raíz de las informaciones recibidas para asegurar la autenticidad de los actos y en caso afirmativo, aplicar las medidas que reparen o eviten al máximo los posibles daños.

d) Presunción de inocencia

Todas las personas afectadas por comunicaciones contarán con su inocencia y honor hasta que quede demostrada fehacientemente a través de las investigaciones llevadas a cabo, lo contrario.

e) Protección de datos personales

Todos los datos personales tratados en virtud del Sistema Interno de Información y sus comunicaciones cumplirán la normativa de protección de datos vigente.

Los datos se conservarán en el sistema de informaciones únicamente durante el tiempo que resulte imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.

Si se acredita que la información facilitada o parte de ella no es veraz, se procederá a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

En todo caso, transcurridos tres (3) meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, se procederá a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema.

La empresa destruirá la información que no sea necesaria conservar o que haya superado el plazo establecido para su conservación. Asimismo, la empresa también dispondrá de un procedimiento de bloqueo, que impedirá el acceso a la información por cualquier persona no autorizada, así como el tratamiento de los datos personales bloqueados.

Atendiendo a los datos a los que la empresa va a tener acceso en virtud de dichas comunicaciones, ésta informará al Informante sobre su deber de conocer y cumplirá con la normativa de protección de datos de carácter personal recogida en la Ley, y en especial la obligación de no divulgar, difundir o hacer uso frente a terceros de información que pueda considerarse de carácter personal a la que tenga acceso.

7. GARANTÍAS DEL SISTEMA INTERNO DE INFORMACIÓN (SII)

7.1. Condiciones de protección

El Sistema Interno de Información, así como el Procedimiento de Gestión de las Informaciones que se reciban a través del canal interno único habilitado, contarán con una serie de garantías, con el objetivo de facilitar tales comunicaciones y defender al Informante en todo momento.

Las personas que comuniquen o revelen infracciones previstas en la definición establecida en el apartado 4.a) tendrán derecho a protección siempre que concurran las siguientes circunstancias:

a) Existan motivos razonables de veracidad de la posible infracción;
b) La comunicación se haya realizado conforme los requerimientos previstos en esta política, así como en la normativa vigente;
c) Se haya realizado con buena fe y,
d) Se encuentre dentro del ámbito de protección de la Ley.

Queda expresamente excluido de la protección prevista en esta política aquellas personas que comuniquen o revelen:

a) Informaciones contenidas en comunicaciones que hayan sido inadmitidas por el canal interno de información por tratarse de:
    a. Hechos relatados que carecen de toda verosimilitud.
    b. Hechos relatados no constitutivos de infracción del ordenamiento jurídico.
    c. Comunicación sin fundamento u obtenida mediante la comisión de un delito.
    d. Comunicación sin 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 que justifiquen un seguimiento distinto.

b) Informaciones 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.

c) Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores.

d) Informaciones que se refieran a acciones u omisiones no comprendidas en el ámbito material de aplicación de la normativa vigente.

Las personas que hayan comunicado o revelado públicamente información sobre acciones u omisiones previstas en el ámbito de aplicación de la ley en cuestión pero que posteriormente hayan sido identificadas y cumplan las condiciones previstas en esta ley, tendrán derecho a la misma protección.

7.2. Prohibición de represalias

En cumplimiento de la normativa vigente, los Informantes que comuniquen mediante el canal habilitado en el Sistema Interno de Información no estarán expuestos a represalias algunas.

El Informante estará protegido frente a las medidas que pudieran adoptarse como represalia durante un plazo de dos (2) años.

8. CANALES EXTERNOS DE INFORMACIÓN

Adicionalmente al canal interno existente en el seno de la organización, resulta relevante destacar la existencia de canales externos de información ante las autoridades competentes y, en su caso, antes las instituciones, órganos u organismos de la Unión Europea.

Concretamente, toda persona física podrá informar ante la Autoridad Independiente de Protección del Informante (A.A.I.) o ante las autoridades u órganos autonómicos correspondientes, de la comisión de cualesquiera acciones u omisiones, ya sea directamente o previa comunicación a través del canal interno detallado.

La información ante la A.A.I. podrá realizarse por escrito, a través de correo postal o a través de cualquier medio electrónico habilitado al efecto dirigido al canal externo de informaciones de la A.A.I., o verbalmente, por vía telefónica o a través de sistema de mensajería de voz. A solicitud del Informante, también podrá presentarse mediante una reunión presencial, dentro del plazo de siete (7) días.

En la fecha de aprobación de esta política y en el ámbito territorial de Cataluña el organismo que realizará la función de A.A.I. es la Oficina Antifrau de Cataluña.

9. ACTUALIZACIÓN Y MEJORA DE ESTA POLÍTICA

La empresa realizará una verificación constante de la aplicación de esta norma y propondrá las oportunas modificaciones en las siguientes circunstancias:

1. Cuando se produzcan cambios legales.
2. Cuando se produzcan cambios en las guías y los criterios de las autoridades de control.

10. FORMACIÓN

Aquellos miembros del Grupo Freixenet que se vean implicados y que sean parte del Sistema Interno de Información recibirán formación sobre el procedimiento a seguir en caso de recepción de una información de cara a cumplir con los requisitos exigidos por la ley, es decir, plazos de contestación, garantía de confidencialidad, no represalias, etc.

11. COMITÉ DE COMPLIANCE

El Comité de Compliance es un comité interno que se ha establecido para supervisar y evaluar la implementación y efectividad de las políticas y procedimientos del Grupo Freixenet en cuanto a su adecuación a la legislación que resulte aplicable en materia de anticorrupción.

12. FORMULACIÓN DE INQUIETUDES Y REPORTE DE INCUMPLIMIENTOS

El Grupo Freixenet quiere ser puntualmente informado de cualquier inquietud que pueda surgir en torno a la presente política, para que pueda afrontar de forma inmediata cualquier posible problema. En caso de duda sobre esta política o alguna inquietud sobre una posible vulneración de la misma, los miembros del Grupo Freixenet deben contactar lo antes posible con su superior jerárquico (de ser aplicable), el Comité de Compliance, el departamento legal o a través del Sistema de Comunicación implementado en el Grupo Freixenet.

El Grupo Freixenet no tolerará represalias de ningún tipo contra aquellos que hayan comunicado, de buena fe, una presunta infracción de las leyes, normas y regulaciones que resulten de aplicación o de las políticas y procedimientos internos del Grupo Freixenet.

13. DIFUSIÓN Y PUBLICIDAD DE LA POLÍTICA

La presente Política del S.S.I. será publicada en la página web y puesta a disposición de todos los empleados junto con el Procedimiento de gestión de las informaciones del Sistema Interno de Información incluido en la misma en el apartado 5.3.

La Organización realizará difusión de la presente Política del S.S.I. y del Procedimiento de gestión de las informaciones del Sistema Interno de Información, con el objetivo de darlo a conocer y fomentar el uso del mismo.

14. APROBACIÓN

La vigente Política Anticorrupción ha sido aprobada por el Consejo de Administración con fecha 12 de junio de 2023, siendo de aplicación obligatoria para todos los empleados del Grupo Freixenet.

ANEXO I: ESTRUCTURA DE CONTROL DEL SISTEMA INTERNO DE INFORMACIÓN

La empresa como ya se ha delimitado anteriormente, dispone de una estructura de control orientada a facilitar la entrada de comunicaciones y garantizar en todo caso la confidencialidad de las mismas. Se basa en el siguiente esquema de trabajo:

Órgano de Administración	Representa el máximo nivel del Sistema Interno de Información, siendo éste el responsable de su implementación previa consulta a la representación legal de los trabajadores, así como el responsable del tratamiento de los datos personales de conformidad con la normativa vigente en protección de datos. Asimismo, le corresponde nombrar a la persona responsable de la gestión de dicho sistema.
Responsable del Sistema Interno	Persona responsable de la gestión del Sistema Interno de Información. Desarrollará sus funciones de manera independiente y autónoma respecto del resto de los órganos de la compañía. Quien ostentará este cargó será el Sr. Thomas Scholl, actual Chief Financial Officer y miembro del Comité de Compliance. En su ausencia ostentará dicho cargo el Sr. Josep Palau, actual Chief Technology Officer y miembro del Comité de Compliance.
Gestores	Personas de referencia que según la materia específica de la que trate la comunicación darán soporte al Responsable del Sistema Interno en llevar a cabo las investigaciones que en su caso resulten pertinentes: • Contabilidad, auditorías y controles financieros internos (irregularidades en la contabilidad y auditoría, mala conducta financiera dentro de los controles interno): Comité de Compliance. • Integridad corporativa (soborno, corrupción y fraude, regalos y hospitalidad, falsificación de documentos, conflictos de interés, competencia y antimonopolio, confidencialidad y violaciones de la protección de datos):

	Comité de Compliance y Delegado de Protección de Datos cuando proceda. • Medio ambiente, salud y seguridad (infracciones de los reglamentos ambientales y de salud y seguridad en el trabajo, incluidas las lesiones corporales y el abuso): Comité Compliance, Responsable Departamento Medio Ambiente y Coordinador de Prevención de Riesgos Laborales cuando proceda. • Recursos Humanos, diversidad y respeto en el lugar de trabajo (discriminación, acoso [sexual] e intimidación, violaciones de derechos humanos, compensaciones, asuntos generales de personal, mala conducta o comportamiento inapropiado): Personas de referencia enumeradas en el Anexo al Protocolo de Acoso en vigor, así como Responsable de Recursos Humanos cuando proceda. • Abuso/malversación de activos o servicios (uso no autorizado de recursos o equipos corporativos por motivos no comerciales, robo de propiedad corporativa, fraude en el horario de trabajo): Comité de Compliance y Responsable de Recursos Humanos cuando proceda. • Otros (otras infracciones de reglas, leyes y directrices, sugerencias generales de mejora y nuevas ideas): Comité de Compliance.