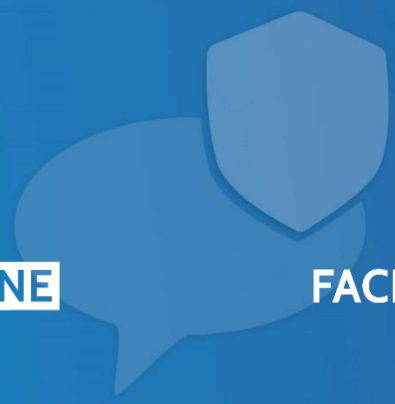
POLÍTICA GENERAL DEL SISTEMA INTERNO DE INFORMACIÓN Y DEFENSA DEL INFORMANTE



CORPORATE LINE
Canal de comunicaciones

FACE to FACE LINE
Canal presencial

cetelem

BNP PARIBAS
PERSONAL FINANCE

ÍNDICE

1 INTRODUCCIÓN

La transposición de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019 al Derecho español 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**, implica la incorporación de instrumentos específicos para que, quienes conocen actuaciones ilegales o irregulares, puedan facilitar datos e información útiles, quedando asegurada una total protección efectiva de dichos informantes.

En este sentido, la citada normativa regula los aspectos mínimos que deben satisfacer los distintos cauces de información internos y externos, junto con el régimen de especial protección de los informantes que actúen con buena fe y conciencia honesta, de forma desinteresada.

De conformidad con lo anterior, EL GRUPO ha implementado un **Sistema Interno de Información (SIIF)**, el cual se configura como un eje fundamental para la supervisión, control y prevención en el ámbito del cumplimiento normativo. Tal sistema constituye un cauce preferente y una herramienta de utilización obligatoria para canalizar la información de manera diligente, a efectos de fortalecer la cultura de la información en el seno de la propia organización.

El SIIF ha sido diseñado como un instrumento de control y de prevención, que contempla los canales de información gestionados tanto internamente como por una empresa externa especializada. Dichos canales gozan de los más altos niveles de profesionalidad, experiencia, independencia, confidencialidad, cumplimiento de la normativa de protección de datos y otros marcos normativos aplicables. Asimismo, el SIIF garantiza los principios básicos de anonimato, adecuado registro, conservación y no alteración, prevención de conflictos de interés, protección del informante y prohibición de represalias.

En atención a la mencionada Ley, es un requisito indispensable que el SIIF cuente con una **Política que enuncie los principios generales del sistema y la defensa del informante**, debidamente publicitada en el seno del Grupo. Por lo tanto, juntamente con el Procedimiento de gestión de las informaciones recibidas, la presente Política es un elemento esencial de la configuración y funcionamiento del SIIF.

2 PRINCIPIOS DE ACTUACIÓN Y GARANTÍAS ESENCIALES

El **Sistema Interno de Información (SIIF)** es uno de los principales ejes de los sistemas de cumplimiento normativo y prevención penal. Atendiendo a las más altas exigencias de diligencia en la materia, el Grupo ha dotado el SIIF de una serie de garantías para asegurar su efectividad, con la colaboración y soporte del experto externo **BONET consulting.** En concreto, los principios básicos y garantías fundamentales que rigen el proceso y la actuación del Grupo en relación con el SIIF son los siguientes:

- **Independencia, autonomía, imparcialidad y ausencia de conflictos de interés:** En la recepción y tratamiento de la información sobre las infracciones se han definido mecanismos de reacción para gestionar y controlar posibles conflictos de interés y/o falta de independencia, cuando los responsables de la gestión, control y/o supervisión presenten una serie de características que comprometan y condicionen el desempeño de sus funciones. Asimismo, todas las comunicaciones recibidas son objeto de análisis con los requisitos necesarios de independencia, que garantizan la equidad y justicia en el tratamiento de éstas.

- **Profesionalidad y experiencia:** Profesionales expertos en cumplimiento normativo, prevención penal y buen gobierno son los encargados del tratamiento y gestión adecuado de las comunicaciones, preservando los derechos de los informantes y los denunciados.

- **Exhaustividad, integridad y confidencialidad de la información:** Los participantes en las distintas fases de investigación tienen el deber de confidencialidad respecto de cualquier información a la que pudieran tener acceso o conocimiento por razón del ejercicio de sus funciones. Además, se impide el acceso a ella por personal no autorizado y se permite un almacenamiento duradero y seguro de la misma, a través de la generación de copias de seguridad de la información y ficheros independientes.

- **Protección de datos y secreto de las comunicaciones:** El tratamiento de datos se ajusta y cumple con las más altas medidas y políticas de protección de datos personales, según la normativa aplicable en materia de Protección de Datos de carácter personal. Del mismo modo, existe el deber de guardar secreto sobre cualquier aspecto relacionado con la información comunicada.

- **Anonimato y Anonimización:** Se prevé la posibilidad de presentación y posterior tramitación de comunicaciones anónimas, así como el deber general de preservar la identidad del informante que se haya identificado al formular la comunicación, manteniéndolo en el anonimato y no revelando su identidad a terceras personas.

- **Uso asequible, simplicidad y gratuidad:** Se garantiza la sencillez en la realización de la comunicación, que permite el acceso universal al sistema sin ningún coste asociado, y la aplicación efectiva de la legalidad y principios éticos que rigen la actividad del Grupo.

- **Registro adecuado e independiente:** Se elabora un libro-registro privado de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar, como garantía de su tratamiento, gestión y no alteración, de forma independiente y sin conflictos de interés, durante un período de tiempo necesario y proporcionado de conformidad con la legislación vigente. En ningún caso los datos se conservarán por un plazo superior a diez años.

- **Prácticas correctas de seguimiento e investigación:** Con la finalidad de comprobar la veracidad de las comunicaciones, la correcta obtención de las evidencias y garantizar los derechos de los afectados, se regulará el ciclo de vida de la comunicación en un procedimiento interno eficaz y transparente. Dichas prácticas estarán documentadas en el Procedimiento de gestión de las informaciones recibidas.

- **Protección del informante y de las personas afectadas:** Las personas que comunican o revelan infracciones tienen derecho a medidas de protección y no serán objeto de ninguna represalia ni consecuencia adversa por su colaboración, incluidas las amenazas de represalia y las tentativas de represalia. De igual forma, las personas afectadas por la comunicación tendrán derecho a la misma protección establecida para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

- **Actuación diligente, responsabilidad y buena fe del informante:** El uso del sistema se asienta en los principios de responsabilidad, diligencia y buena fe, por lo que todo informante debe tener motivos razonables para pensar que la información es veraz en el momento de su comunicación. La comunicación de hechos infundados, falsos o tergiversados, así como la remisión de informaciones obtenidas de manera ilícita, con actitud maliciosa y moralmente deshonesta, supone una infracción del principio de buena fe y puede derivar en la aplicación de medidas disciplinarias.

3 RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN

Para la eficacia del **Sistema Interno de Información (SIIF)** resulta indispensable la designación de un responsable de su correcto funcionamiento, organización y tramitación diligente de las informaciones. Asimismo, éste se encargará de asegurar la debida comunicación y difusión del SIIF, así como de realizar y actualizar el pertinente plan de formación.

El órgano de administración u órgano de gobierno del Grupo es el competente para la designación y comunicación a la autoridad competente, de la persona física u órgano colegiado responsable de la gestión de dicho sistema y de su destitución o cese (en adelante, el **Responsable del Sistema**).

El Responsable del Sistema desarrolla sus funciones de forma **independiente y autónoma** respecto del resto de los órganos de organización del Grupo, evitando posibles situaciones de conflicto de interés con el desempeño ordinario de su cargo. No obstante, el Responsable del Sistema puede recurrir a otros terceros para recibir soporte especializado y/o cumplir con los requisitos de independencia, para asegurar el debido el desempeño de sus funciones.

Especialmente, para el ejercicio de sus funciones el Responsable del Sistema se coordinará con los siguientes sujetos:

A El responsable de recursos humanos, cuando pudiera proceder la adopción de medidas disciplinarias contra las personas implicadas y/o coordinar la aplicación de medidas de protección.

B Los responsables de cumplimiento normativo y/o de los servicios jurídicos del Grupo, si procediera la adopción de medidas de carácter legal o de cumplimiento normativo que deben ser tomadas en consideración, por estos, en relación con las comunicaciones recibidas en el SIIF.

C Los encargados del tratamiento que eventualmente se designen.

D El Delegado / Responsable de Protección de Datos.

E Otras personas y/o entidades intervinientes en la gestión del SIIF.

4 AUTORIDAD INDEPENDIENTE DE PROTECCIÓN DEL INFORMANTE

El **Sistema Interno de Información (SIIF)** del Grupo es el medio prioritario y de utilización obligatoria para la comunicación de conductas ilícitas o infracciones de las que se tenga conocimiento, pues permite asegurar la debida adopción de medidas de protección y fomentar la cultura de la información dentro de la organización.

No obstante, se han determinado otros canales de información "externos", con el fin de ofrecer a los ciudadanos una alternativa donde presentar la comunicación y/o reclamación, en los supuestos que los canales internos no cumplan con las garantías exigidas por la normativa aplicable, no se apliquen las pertinentes medidas de protección o las personas sean expuestas a represalias por su condición de informantes.

Por consiguiente, toda persona física puede informar directamente a la **Autoridad Independiente de Protección del Informante, A.A.I.** de la comisión de cualesquiera acciones u omisiones constitutivas de infracción del ordenamiento jurídico, a través del canal externo de información de dicha autoridad pública especializada. El acceso a dicho canal de información externo y los datos de contacto de la Autoridad se encuentran publicados en su página web.

5 CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES

Los tratamientos de datos personales que derivan del **Sistema Interno de Información (SIIF)** se rigen por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre y en la Ley Orgánica 7/2021, de 26 de mayo. Por ello, en el momento de la captación, los interesados son informados del tratamiento de sus datos y de sus derechos, de acuerdo con la normativa vigente.

En cumplimiento del principio de **minimización de datos**, los datos de carácter personal recopilados son aquellos necesarios y pertinentes para el tratamiento de la comunicación. En el supuesto de que se recopilen datos por accidente, que no sean necesarios para el conocimiento e investigación de las acciones u omisiones, estos serán eliminados sin dilación indebida. Asimismo, los datos se conservarán durante el tiempo imprescindible para decidir sobre la precedencia de iniciar una investigación.

Por otro lado, el diseño del SIIF garantiza la **confidencialidad** de la identidad del informante y de cualquier tercero mencionado en la comunicación, así como de las actuaciones desarrolladas en la gestión y tramitación de la misma. En este sentido, el acceso a los datos personales y el resto de información contenida en el sistema está limitada a los responsables de la gestión, dentro del ámbito de sus competencias y funciones. Por lo tanto, se dispone de medidas técnicas y organizativas adecuadas para preservar la identidad de los afectados e impedir el acceso de personas no autorizadas.

En el caso de cualquier duda o consulta sobre el tratamiento de datos de carácter personal llevado a cabo en el seno de las entidades del Grupo en relación con el SIIF, todo interesado puede dirigirse al **Delegado / Responsable de Protección de Datos** designado, a través de los datos de contacto que le han sido previamente comunicados y que están a su disposición.

6 MEDIDAS DE PROTECCIÓN

Las personas que comuniquen o revelen infracciones utilizando el **Sistema Interno de Información (SIIF)** del Grupo tienen **derecho a protección**, en las mismas condiciones que quienes informen por canales externos, siempre que 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.

En este sentido, se prohíben expresamente los actos constitutivos de **represalia**, incluida la amenaza y tentativa, contra las personas que presenten una comunicación. Se entiende por represalia:

a Actos u omisiones prohibidos por la ley.

b Actos u omisiones que de forma directa o indirecta supongan un trato desfavorable, situando a la persona en desventaja con respecto a otra.

A título enunciativo y no limitativo, se consideran represalias:

- Suspensión del contrato de trabajo, despido o extinción de la relación, terminación anticipada, anulación del contrato de trabajo y/o mercantil, medidas disciplinarias, amonestación u otra sanción, degradación o denegación de ascensos, modificación sustancial de las condiciones y no conversión del contrato temporal en indefinido o medidas equivalentes.
- Daños (incluidos reputacionales), pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.
- Evaluación o referencias negativas sobre el desempeño laboral o profesional.
- Listas negras o difusión de información que dificulte o impida el acceso a empleo / contratos de obras o servicios.
- Denegación o anulación de licencia o permiso.
- Denegación de formación.
- Discriminación, trato desfavorable o injusto.
- Denegación de incentivos, beneficios, bonos, comisiones y cualquier otro tipo de compensación.
- Terminación anticipada, suspensión, alteración o anulación de contratos de bienes o servicios.

Estos actos serán nulos de pleno derecho y darán lugar, en su caso, a medidas correctoras disciplinarias o de responsabilidad, pudiendo incluir la correspondiente indemnización de daños y perjuicios al perjudicado.

A efectos de garantizar el derecho de protección del informante y el de las personas afectadas por la comunicación, el Grupo tiene establecidas las siguientes medidas técnicas y organizativas las cuales se aplican desde el momento inicial en el que se recibe la comunicación:

1. **Configuración del SIIF:** El SIIF se ha diseñado con las medidas técnicas y organizativas adecuadas para garantizar la protección de la identidad del informante, así como de aquellos datos e informaciones que se deriven de las comunicaciones presentadas. En este sentido, el Grupo ha habilitado una serie de canales internos de información, los cuales permiten presentar comunicaciones de forma anónima. Dichos canales son:

   - **Canal on-line / digital:** Plataforma digital para la presentación de comunicaciones por escrito.
   - **Canal presencial / "face to face":** El Sistema de recepción de comunicaciones mediante reunión presencial o por videoconferencia.

   Con independencia del canal que se utilice, el SIIF garantiza la aplicación efectiva de los principios básicos y garantías especificadas en la presente Política, a fin de cumplir con los requisitos del marco normativo y proteger los derechos de los informantes y las personas afectadas.

2. **Responsable del SIIF:** Para asegurar la debida aplicación del SIIF, el Grupo tiene designado a un Responsable cuya función radica en la supervisión, vigilancia y control del funcionamiento del mismo. En este sentido, el Responsable, junto con el experto externo, adoptarán las medidas de protección necesarias y velarán por su debido seguimiento y aplicación. La participación del experto externo dota a las funciones del Responsable de los elementos de autonomía e independencia requeridos por la normativa vigente.

   Asimismo, el Responsable será el encargado de realizar un análisis preliminar de las comunicaciones recibidas a efectos de determinar la idoneidad de adoptar medidas de protección específicas respecto al informante y/o terceros afectados. Además, en función de la naturaleza y alcance de la información, el Responsable contará con el apoyo y asesoramiento de los responsables de las diferentes áreas operativas del Grupo, para el buen fin de la investigación. También podrá recurrir a otros terceros especializados en aquellas materias que requieran una opinión experta.

3 **Custodia, gestión y seguridad de la información del SIIF:** El Grupo dispone de un sistema de gestión documental configurado con las medidas apropiadas de seguridad y control, a efectos de evidenciar la propia eficacia del SIIF. Cabe destacar que dicho sistema incluye procesos de anonimización, a fin de no permitir la identificación de los informantes. Adicionalmente, el Grupo ha adoptado medidas técnicas razonables para la conservación, recuperación y eliminación de manera segura de la información, así como la implantación de controles de acceso para impedir el uso no autorizado.

Sin embargo, quedan excluidas de la mencionada protección las informaciones remitidas que sean falsas, tergiversadas, carezcan manifiestamente de toda verosimilitud y fundamento o existan indicios racionales de haberse obtenido mediante la comisión de un delito. Esto es debido a que todas las comunicaciones deben realizarse bajo el principio de **buena fe** y, por tanto, el informante debe tener motivos razonables para pensar que la información es veraz en el momento de la comunicación. En resumen, el principio de buena fe requiere que en ningún caso pueda desprenderse que existe falsedad, falta a la verdad, intención de venganza o de perjudicar a un tercero.

Es importante recordar que las medidas de protección no se dirigen sólo a favor de los informantes. También aquellas personas a las que se refieran los hechos relatados en la comunicación (**personas afectadas**) cuentan con una singular protección ante el riesgo de que la información, aún con aparentes visos de veracidad, haya sido manipulada, sea falsa o responda a otras motivaciones. Durante la tramitación del expediente, estas personas tienen derecho a la presunción de inocencia, a la tutela judicial y defensa, al acceso al expediente, así como a la confidencialidad de los hechos y datos del procedimiento y a la reserva de su identidad. En conclusión, tienen la misma protección y derechos que goza el informante.

7 RÉGIMEN DISCIPLINARIO

El incumplimiento de la normativa aplicable y las conductas contrarias a las instrucciones, políticas, códigos, procedimientos y protocolos del Grupo es motivo de aplicación del **régimen disciplinario a nivel laboral y mercantil**, en coordinación con lo establecido en el Convenio Colectivo de aplicación, el Estatuto de los Trabajadores y el resto de las normas aplicables.

El Grupo notificará y sancionará las acciones u omisiones contrarias a la presente Política en las que incurran los empleados, colaboradores o cualquier miembro relacionado con el Grupo y, en particular:

- La no comunicación de cualquier sospecha o conocimiento de infracciones e incumplimientos del marco normativo y de los protocolos y normas internas del Grupo a través del SIIF.
- Cualquier intento o acción efectiva de obstaculizar la presentación de comunicaciones o impedir, frustrar o ralentizar su seguimiento.
- La utilización del SIIF de mala fe, por ejemplo, con la aportación de información o documentación a sabiendas de su falsedad.
- La adopción de cualquier represalia derivada de la comunicación frente a los informantes o las demás personas afectadas.
- La vulneración de las garantías de confidencialidad y anonimato, revelando la identidad de las personas afectados y quebrantando el deber de secreto de las informaciones.
- El incumplimiento de la obligación de colaboración con la investigación de informaciones.

8 COMUNICACIÓN, REVISIÓN Y ACTUALIZACIÓN

La presente Política, así como toda la información necesaria sobre el uso del **Sistema Interno de Información (SIIF)** implantado, está disponible en una sección separada y rápidamente identificable, para que todos los interesados la tengan a su alcance de forma clara y fácilmente accesible. No obstante, cualquier persona puede solicitar información adicional al Grupo a través de los datos de contacto del Responsable.

El **Responsable del Sistema** revisará periódicamente y, en su caso, propondrá al órgano de administración u órgano de gobierno del Grupo la actualización de la presente Política, con la finalidad de adaptarla a todas aquellas circunstancias y cambios que puedan ir surgiendo, así como a la normativa o jurisprudencia que pueda dictarse. Todo ello, con el objetivo de adecuar el SIIF a las máximas exigencias de cumplimiento normativo para su correcto funcionamiento y eficacia.

Asimismo, el Grupo está abierta a cualquier **sugerencia y/o propuesta** que pueda mejorar su actuación ética y favorecer una cultura de cumplimiento normativo, remarcando la necesidad de que todos los empleados y miembros relacionados el Grupo o terceros colaboren para cumplir con sus valores y principios.

9 CANALES INTERNOS DE INFORMACIÓN

A efectos de cumplir con las disposiciones recogidas en la Ley 2/2023, el Grupo tiene implementado un sistema configurado con los requisitos técnicos y procedimentales requeridos por dicha Ley para la debida atención de las comunicaciones. Todo ello con la finalidad de ofrecer a los informantes un entorno de comunicación seguro, confidencial o incluso anónimo con el Grupo, y tramitar las informaciones de forma eficiente, profesional e independiente.

Para ello, el Grupo se ha dotado de recursos materiales, técnicos y humanos para habilitar distintos canales internos que permiten la presentación de comunicaciones en formato escrito o verbal. Dichos canales cuentan con la configuración, diseño y soporte de un experto externo en aras de aportar los más altos niveles de profesionalidad, experiencia, independencia, confidencialidad, protección de datos y del informante, y otros ámbitos aplicables para este tipo de canales.

Cabe destacar que, la información proporcionada mediante cualquiera de los canales internos será tratada de manera confidencial, y solo tendrá acceso a la misma el personal autorizado para su debida gestión y tramitación.

A continuación, se detallan los canales de los que dispone cualquier empleado o tercero vinculado con el Grupo para la presentación de las comunicaciones:

Canal On-line/Digital

CORPORATE LINE
Canal de comunicaciones

El Grupo dispone de una herramienta digital que permite presentar comunicaciones por escrito mediante un formulario, el cual permite adjuntar archivos. Una vez cumplimentado el formulario, la herramienta genera automáticamente un código que permite el debido seguimiento y gestión por parte del responsable de la tramitación. Asimismo, se envía una confirmación al informante respecto a la entrada y registro de la comunicación en el sistema, la cual contiene un resumen de la información aportada, así como el código para que éste también pueda realizar dicho seguimiento.

Esta herramienta cuenta con medidas de seguridad que garantizan la protección de la información, la identidad del informante y la de aquellas personas afectadas por la misma, así como la confidencialidad y reserva de todo el proceso de gestión y tramitación de la comunicación. En este sentido, el Grupo garantiza un entorno de comunicación seguro y diligente para la recepción de comunicaciones.

La herramienta también permite la presentación de comunicaciones de forma anónima. Gracias al sistema de comunicación y seguimiento que dispone, el informante y el Responsable del Sistema podrán comunicarse a través de la herramienta, con independencia de si la comunicación se ha presentado anónimamente.

El enlace de acceso a esta herramienta y su ámbito de uso está disponible en la página web del Grupo.

Canal Presencial / "Face to face"

Otra de las vías que el Grupo pone a disposición de sus empleados y aquellos terceros que se relacionan con ésta es el canal presencial / "face to face", cuya finalidad es la de permitir la presentación de comunicaciones verbales mediante una reunión presencial o por videoconferencia. En este caso, y teniendo en cuenta la complejidad que conlleva para el Grupo garantizar el anonimato del informante en aquellos casos que así se solicite, el Grupo ha encomendado esta función al experto externo BONET consulting, el cual se encarga de recibir y gestionar las comunicaciones con estas características, así como aquellas otras en las que se identifiquen los informantes y se requiera la gestión presencial. En este sentido, el experto externo garantiza la protección de la identidad del informante tanto en el proceso de solicitud de cita previa, en la presentación de una comunicación en formato presencial, como en el lugar de realización de la misma.

A efectos de garantizar la seguridad y preservar la integridad de la información que aporte el informante, la reunión será grabada conforme a lo estipulado en la Ley y con el consentimiento previo del informante. Dicha reunión quedará documentada en un formato seguro, con las medidas de seguridad y anonimización requeridas por el marco normativo. En esta línea, BONET consulting dispone y habilitará los mecanismos tecnológicos necesarios para el envío de documentación complementaria a la información aportada en la reunión.

Para poder hacer uso de este canal, el Grupo ha habilitado un teléfono y un correo electrónico de contacto para solicitar la presentación de comunicaciones en este formato, cuya atención y coordinación de la reunión será realizada exclusivamente por BONET consulting. Los datos de contacto para realizar esta solicitud están debidamente publicados en la página web del Grupo.

De manera alternativa, el Grupo BNP Paribas pone a disposición de los usuarios otros canales de información gestionados por el propio Grupo, los cuales quedan fuera del ámbito de aplicación de la presente Política.

COPYRIGHT