

Procedimiento de Gestión de Informaciones

Índice

1 OBJETO.....	3
2 ÁMBITO DE APLICACIÓN	3
3 RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN.....	5
4 CANALES INTERNOS DE INFORMACIÓN	5
5 TRAMITACIÓN DE LAS INFORMACIONES	6
5.1 RECEPCIÓN DE INFORMACIONES	6
5.2 ANÁLISIS PRELIMINAR DE INFORMACIONES	7
5.3 COMISIÓN DE INVESTIGACIÓN / CI	8
5.4 DILIGENCIAS DE INVESTIGACIÓN	9
5.5 CONCLUSIONES DE LAS ACTUACIONES.....	10
6 CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES	12
7 SEGUIMIENTO Y REPORTING	13
8 COMUNICACIÓN Y FORMACIÓN	13
9 ENTRADA EN VIGOR	14
ANEXO I MEDIDAS DE PROTECCIÓN	15



1 OBJETO

GRUPO CETELEM (en adelante, "El Grupo"), en su compromiso por fortalecer una cultura de la información como mecanismo para prevenir y detectar amenazas al interés público, tiene implementado un Sistema Interno de Información (en adelante, "SIIF"). En cumplimiento del artículo 9 de 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, el Grupo ha desarrollado el presente procedimiento de gestión de las informaciones que se comuniquen a través del Sistema Interno de Información.

En este sentido, el presente documento tiene por objeto establecer el procedimiento de recepción, gestión, tratamiento, investigación y resolución de comunicaciones relativas a indicios, sospechas o evidencias de posibles incumplimientos normativos, delitos e incumplimientos de los protocolos, normas y códigos internos del Grupo, que se reciban mediante los canales internos de información habilitados a tal efecto.

2 ÁMBITO DE APLICACIÓN

Este procedimiento es de aplicación a los gestores, responsables, colaboradores y otros terceros implicados en la gestión del Sistema Interno de Información del Grupo. En este sentido, se establece este procedimiento para garantizar la diligencia de las actuaciones en la tramitación de las comunicaciones por parte de los sujetos designados a tal efecto, asegurando la confidencialidad de la información, anonimato y la protección de la identidad de la persona que informa, así como la de aquellas personas afectadas o cualquier otro tercero mencionado en las comunicaciones.

A través del SIIF se podrán comunicar las acciones u omisiones previstas en el artículo 2 de la Ley 2/2023:

- Infracciones del Derecho de la Unión Europea (UE) siempre que entren dentro del ámbito de aplicación de los actos de la UE enumerados en el anexo de la Directiva 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019 y que afecten a los intereses financieros de la UE o incidan en el mercado interior.

- En el ámbito del ordenamiento jurídico español, las infracciones penales, las infracciones administrativas graves y muy graves y las infracciones del Derecho Laboral en materia de seguridad y salud en el trabajo.
- Otras infracciones de procedimientos, políticas, manuales y códigos internos del Grupo



BNP PARIBAS

**The bank
for a changing
world**

3 RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN

El órgano de administración u órgano de gobierno del Grupo ha designado a un Responsable del Sistema Interno de Información encargado de la gestión de dicho sistema, la tramitación de los expedientes de investigación, la debida comunicación y difusión del SIIF, así como la programación y actualización del pertinente plan de formación al respecto.

En el marco de sus funciones, el Responsable del Sistema tiene que actuar 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. Asimismo, el Responsable podrá designar a un responsable o equipo operativo, interno o externo, como soporte a sus funciones. En tales circunstancias, dichas personas deberán estar formalmente designadas y conocer debidamente el contenido del presente documento.

En cuanto a la gestión de las informaciones y tramitación de los expedientes de investigación, el Responsable del Sistema también podrá recurrir a otros terceros o responsables internos para recibir soporte especializado y/o cumplir con los requisitos de independencia, para asegurar el debido el desempeño de sus funciones. Especialmente, el Responsable del Sistema se podrá coordinar con los siguientes sujetos:

- 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.
- 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.
- Los encargados del tratamiento que eventualmente se designen.
- El Delegado / Responsable de Protección de Datos.
- Otras personas y/o entidades que por su perfil, conocimiento o experiencia pudieran participar en la tramitación y gestión en los expedientes de investigación.

4 CANALES INTERNOS DE INFORMACIÓN

A efectos de cumplir con las disposiciones recogidas en la Ley 2/2023, del Grupo ha desarrollado una Política General sobre el Sistema Interno de Información. En dicha política se detallan los Canales Internos de Información habilitados por el Grupo para informar sobre las acciones u omisiones previstas en el apartado 2 del presente documento.

En este sentido, el Grupo se ha dotado de los recursos materiales, técnicos y humanos necesarios para configurar debidamente estos canales y permitir la presentación de comunicaciones en formato escrito o verbal. Asimismo, 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.

La descripción y acceso a los canales se encuentra debidamente detallado en la Política General del Grupo.

5 TRAMITACIÓN DE LAS INFORMACIONES

5.1 RECEPCIÓN DE INFORMACIONES

El presente procedimiento se activará en el momento en que se reciba una comunicación en el Sistema Interno de Información (SIIF) y su puesta en conocimiento del Responsable del Sistema a través de los siguientes canales:

1. **Canal On-line / Digital:** El Responsable del SIIF se encargará de dar lectura y analizar la comunicación en el momento que la herramienta detecte su entrada y reciba la notificación al respecto. En caso de delegación en otros equipos o responsables operativos, asignados como gestores del Canal, éstos informarán inmediatamente al Responsable del SIIF de las comunicaciones recibidas.
2. **Canal Presencial / "Face to face":** BONET consulting, experto externo encargado de la gestión de las solicitudes de cita previa para la presentación de comunicaciones en formato presencial, atenderá al informante y señalará la fecha, hora y lugar de la reunión, en coordinación con el Responsable del SIIF.

Una vez recibida la comunicación, el Responsable del SIIF o el responsable/equipo operativo que haya designado a tal efecto, enviará acuse de recibo de la misma al informante en el plazo de 7 días naturales a su recepción, salvo que la comunicación sea presentada por una vía distinta a los canales oficiales habilitados por el Grupo que pudiera poner en peligro la

confidencialidad de la comunicación, y se deberá justificar debidamente el motivo por el cual no se otorga dicho acuse.

5.2 ANÁLISIS PRELIMINAR DE INFORMACIONES

Tras recibir la información, el Responsable del SIIF realizará un análisis preliminar del contenido de la comunicación, así como de los ficheros o documentos adjuntados en relación con los hechos informados. En este sentido, se evaluarán de forma pormenorizada las manifestaciones presentadas al objeto de valorar su alcance, veracidad y pertinencia y, complementariamente, la implicación de potenciales afectados, respetando en todo momento la privacidad, la confidencialidad, la presunción de inocencia y el honor de los afectados.

Dicho análisis podrá generar los siguientes resultados:

- 1 Admisión de la comunicación:** Cuando la información esté comprendida dentro del ámbito del SIIF, por estar los hechos descritos relacionados con potenciales incumplimientos normativos o por tratarse de acciones u omisiones contrarias a los principios y valores del Grupo, establecidos en sus protocolos, normas y códigos de conducta.

En este supuesto, el Responsable del SIIF analizará e identificará las personas objeto de protección y las medidas de protección necesarias a adoptar frente a posibles represalias, tomando como base las recogidas en el ANEXO I del presente documento, pudiéndose configurar a medida según el caso concreto. En este sentido, el Responsable realizará un seguimiento periódico de la situación del informante y, en su caso, de aquellas personas incluidas en el régimen de protección.

Con el fin de decidir sobre la admisión a trámite de la comunicación, se prevé la posibilidad de que el Responsable pueda solicitar al informante la aclaración o complemento de los hechos comunicados.

- 2 Inadmisión de la comunicación:** Cuando la valoración previa de la información concluya que los hechos descritos son de una naturaleza distinta a los comentados anteriormente, así como cuando la comunicación haya sido interpuesta de mala fe, con actitud maliciosa y moralmente deshonesto o verse sobre hechos infundados, falsos o tergiversados.

En función de la decisión tomada por el Responsable del SIIF, se procederá a abrir el expediente de investigación o al archivo de la información, documentando los motivos que han llevado a la admisión / inadmisión de la misma. En ambos casos, se informará por escrito al informante de la decisión adoptada, salvo que se hubiera utilizado canales distintos que no contemplen las garantías de protección del Sistema Interno de Información. En todo caso, el Responsable documentará debidamente las decisiones adoptadas al respecto.

Con todo, la infracción del principio de buena fe podrá derivar en la aplicación de medidas disciplinarias al informante, por lo que se trasladará esta circunstancia y la propuesta de sanción al equipo competente para determinar la acción disciplinaria a aplicar al informante de mala fe.

5.3 COMISIÓN DE INVESTIGACIÓN / CI

En el caso de admisión a trámite de la información presentada, el Responsable del Sistema será el encargado de crear la Comisión de Investigación (en adelante, la "CI") en función de los parámetros y elementos a investigar identificados en el análisis preliminar.

En cuanto a la composición de dicha Comisión, atendiendo a lo comentado anteriormente, podrá ser de tres tipos:

- **Comisión de Investigación Interna (CIIN):** configurada únicamente por personal interno del Grupo.
- **Comisión de Investigación Mixta (CIMX):** configurada por personal interno del Grupo con el soporte de expertos externos.
- **Comisión de Investigación Externa (CIEX):** configurada en exclusiva por expertos externos.

Por cada información admitida a trámite se activará el proceso de creación de la CI cuyos miembros podrán variar en cada caso. A tal efecto, todos los miembros de la CI deberán firmar el correspondiente documento sobre el compromiso y obligación de guardar la máxima reserva y secreto sobre la información que reciba, acceda o tuviera conocimiento como miembro de la comisión de investigación, dado que toda esta información es clasificada como "confidencial".

Para la designación de los miembros de la Comisión de Investigación, se evaluará la idoneidad de sus perfiles bajo los criterios de experiencia profesional y formación, según la materia objeto de investigación. Asimismo, deberán contar con formación y soporte en procesos de investigación y entrevistas. Por otro lado, se analizará si concurre alguna incompatibilidad o conflicto de interés, en cuyo caso, se propondrá la designación de otro miembro.

Durante el proceso de investigación, se podrá modificar la composición de la CI en caso de que se requiera la incorporación de un nuevo miembro, o cese de uno existente, según las necesidades del proceso. En todo caso se contemplarán los criterios de idoneidad de los perfiles comentados en el párrafo anterior.

Si fuera preciso, la CI podrá solicitar soporte a expertos externos especializados en aquellas diligencias de investigación que se precise, los cuales actuarán bajo los principios de actuación y garantías recogidas en la Política General del Sistema Interno de Información y Defensa del Informante desarrollada por el Grupo. En este sentido, el proceso de contratación de dichos terceros se llevará a cabo con la celeridad necesaria al objeto de cumplir con los plazos de investigación definidos en la Ley 2/2023.

5.4 DILIGENCIAS DE INVESTIGACIÓN

Una vez constituida la Comisión de Investigación, se dará apertura a un expediente de investigación y se practicarán aquellas diligencias que se estimen oportunas para comprobar la verosimilitud de los hechos informados. Todo ello quedando debidamente registrado en el SIIF del Grupo. Algunas de las principales diligencias que podrán conformar la investigación son:

- Entrevistas personales con el informante, personas afectadas por las informaciones y cualquier otro tercero que se mencione o tenga implicación en las mismas.
- Recabar toda la documentación que se estime necesaria procedente de cualesquiera niveles de organización del Grupo.
- Solicitar informes, dictámenes periciales o cualesquiera otros medios de prueba que se considere oportunos.

El plazo de investigación no podrá exceder los (3) meses a contar desde la recepción de la comunicación o, si no se ha remitido un acuse de recibo al informante, a tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación, salvo casos

de especial complejidad que requieran una ampliación de plazo, en cuyo caso, este podrá extenderse hasta un máximo de otros (3) meses adicionales.

En el proceso de una investigación, el Responsable del Sistema, o el responsable/equipo operativo asignado a tal efecto, podrá solicitar al personal del Grupo su colaboración en las diligencias de investigación. A este respecto, las personas afectadas por la comunicación tendrán la obligación de comparecer y contestar a todos los requerimientos de entrevistas, información o documentación formulados por el Responsable.

En este sentido, las personas afectadas tendrán derecho a la presunción de inocencia, al derecho de defensa y al derecho de acceso al expediente en los términos regulados en esta ley, así como a la misma protección establecida para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento. Asimismo, tendrán la obligación de mantener la confidencialidad sobre todo el contenido y acciones realizadas en el marco de la investigación.

Asimismo, las personas afectadas serán informadas de los hechos que se le pudieran atribuir en el momento y forma que la CI considere adecuados para garantizar el buen fin de la investigación, tendrán derecho a ser oídas para exponer su versión de los hechos y aportar aquellos medios de prueba que considere oportunos. En ningún caso se les comunicará la identidad del informante ni tendrá acceso a la comunicación.

5.5 CONCLUSIONES DE LAS ACTUACIONES

Finalizadas todas las diligencias de investigación, la Comisión de Investigación emitirá un informe de conclusiones que contendrá como mínimo los siguientes aspectos:

- A** Una exposición de los hechos relatados junto con el código de identificación de la comunicación y la fecha de registro.
- B** Las actuaciones realizadas con el fin de comprobar la verosimilitud de los hechos.
- C** Medidas adoptadas en relación con el informante, los afectados y otros terceros implicados en la comunicación.
- D** Las conclusiones alcanzadas en la instrucción y la valoración de las diligencias y de los indicios que las sustentan.

Una vez emitido el informe de investigación, la CI revisará las pruebas y las conclusiones alcanzadas en dicho informe, y decidirá motivadamente:

- A** Archivo del expediente por no constituir la conducta investigada una infracción de las contempladas en el ámbito de aplicación de la Ley 2/2023 o por falta de colaboración por parte de las personas afectadas por la comunicación.
- B** Apertura de un procedimiento sancionador, dando traslado de las actuaciones realizadas al Órgano del Grupo competente de aplicar el Régimen disciplinario correspondiente.
- C** Plan de desarrollo y actualización de medidas formativas y procedimientos de control en materia de cumplimiento normativo y prevención penal a adoptar por el Grupo mitigar o prevenir las conductas o hechos analizados en el expediente.
- D** Comunicación de las implicaciones y aspectos a considerar en otras áreas y/o responsables de cumplimiento normativo del Grupo, si fuera necesario realizarlo de manera complementaria.
- E** Remisión al Ministerio Fiscal o a los órganos judiciales pertinentes si la conducta sea constitutiva de una infracción penal, o a la Fiscalía de la Unión Europea en caso de que se vean afectados los intereses financieros de la Unión Europea.

Una vez finalizado el proceso de investigación, se notificará al informante sobre las medidas de seguimiento previstas, así como el resultado de las investigaciones, debiendo motivar la razón por la cual se han adoptado las medidas o acciones disciplinarias. En caso de que se acuerde el archivo del expediente, será notificado al informante y, en su caso, a la persona afectada.

Si de las diligencias de investigación realizadas se acredita que los hechos informados son falsos, tergiversados o se han obtenido de manera ilícita, el informante será sancionado de conformidad con el Régimen sancionador aplicable del Grupo.

6 CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES

En el marco de gestión del Sistema Interno de Información del Grupo, el acceso a los datos personales quedará limitado exclusivamente a quienes desarrollen las funciones de gestión del Sistema, o a los encargados de tratamiento que eventualmente se designen a tal efecto (véase punto 3 Responsable del Sistema Interno de Información).

Será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales o administrativos que, en su caso, procedan. No obstante, si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de los mismos. Asimismo, si se acreditara que la información facilitada o parte de ella no es veraz, no es necesaria o pertinente para la investigación, deberá procederse a su inmediata supresión, 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.

Los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados. 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. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada.

La identidad del informante solo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.

Durante todo el procedimiento de gestión de las informaciones es necesario aplicar las medidas técnicas y organizativas necesarias para garantizar la autenticidad e inalterabilidad de los datos y las informaciones en todas sus fases del tratamiento. Es decir, desde la recogida inicial, el procedente traslado, el análisis previo, el proceso de investigación y la resolución, hasta la custodia y conservación de la información en el sistema de almacenamiento.

En particular, los datos y las informaciones protegidas abarcan aquellas contenidas en la comunicación, las pruebas recabadas con posterioridad y los datos a los que se tenga acceso a raíz de la apertura del expediente de investigación, incluidos todos los ficheros y documentos relacionados con los hechos informados y las grabaciones de las entrevistas realizadas con cualquier persona implicada.

Por ende, el sistema de almacenamiento y custodia de la documentación debe estar dotado de las medidas de seguridad adecuadas para el debido registro, control, seguimiento y conservación de las informaciones de conformidad con lo estipulado por el marco normativo aplicable.

Contemplado lo anterior, el Responsable del SIIF en coordinación con el Delegado/Responsable de Protección de Datos analizarán e identificarán los mecanismos de seguridad, ubicaciones y procedimientos de control necesarios a efectos de garantizar la debida confidencialidad de la información y protección de todos los datos en relación con el presente procedimiento. Dicho esquema de seguridad y protección estará debidamente documentado y formará parte del SIIF.

7 SEGUIMIENTO Y REPORTING

El Responsable del Sistema será el encargado de revisar periódicamente y, en su caso, propondrá al Órgano de Gobierno del Grupo, la actualización del presente procedimiento con la finalidad de adaptarlo a todas aquellas circunstancias y cambios que puedan ir surgiendo, así como a la normativa o jurisprudencia que pudiera dictarse. Todo ello al objeto de adecuar el SIIF a las máximas exigencias de cumplimiento normativo para su correcto funcionamiento y eficacia conforme a la Ley 2/2023.

Asimismo, el Responsable del Sistema será el encargado de elaborar un informe de actividad del SIIF, incluyendo el seguimiento efectuado a las informaciones / denuncias recibidas, señalando, si procediera, la investigación llevada a cabo, información sobre el origen y motivo de la denuncia, entre otros. Dicho informe deberá ser reportado al Órgano de Gobierno con carácter anual o, en su defecto, cuando sea requerido por dicho órgano.

8 COMUNICACIÓN Y FORMACIÓN

Para la debida aplicación del procedimiento de gestión de informaciones, el Responsable del SIIF elaborará un Plan de formación que deberá contemplar el siguiente alcance:

- Formación específica y avanzada para el Responsable del SIIF, y el responsable/equipo operativo que se designe, como personal encargado de aplicar el presente procedimiento.
- Formación complementaria para aquellos sujetos que pudieran participar como colaboradores en los procesos de investigación.

De forma complementaria, el Responsable del SIIF deberá asegurar la debida comunicación y difusión del presente procedimiento a aquellas personas que se designen como gestores del Sistema y a los responsables internos de otras áreas de actividad del Grupo en materia de cumplimiento normativo.

Asimismo, se diseñará un plan de comunicación con objeto de trasladar a los empleados y terceros vinculados con el Grupo el deber de utilización del Sistema Interno de Información para informar sobre acciones u omisiones que puedan constituir infracciones o incumplimientos normativos de las que tengan conocimiento, así como el deber de colaboración cuando sea requerido por el Responsable del SIIF. Todo ello en los términos establecidos en la Política General del Sistema del Grupo.

Contemplado lo anterior, el Responsable del SIIF llevará a cabo un registro documentado de los planes de formación y comunicados realizados al respecto.

9 ENTRADA EN VIGOR

El contenido del presente procedimiento es de obligado cumplimiento para todos los destinatarios del mismo desde el momento que se proceda a su comunicación, debiéndolo de aceptar y cumplir en todos sus términos.

Se mantendrá vigente hasta que sea modificado o sustituido, y debidamente aprobado y ratificado por el Órgano de Gobierno del Grupo, entrando en vigor desde el momento que se proceda a su comunicación.

ANEXO I MEDIDAS DE PROTECCIÓN

Las personas que comuniquen o revelen infracciones utilizando el Sistema Interno de Información 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.

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.

Complementariamente a lo expuesto, se deberán incorporar las medidas protección necesarias a las personas a las que se refieran los hechos relatados en la comunicación (personas afectadas), las cuales también 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. Dichas personas son:

- A** Personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso,
- B** Personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante, y
- C** Personas jurídicas, para las que trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa. A estos efectos, se entiende que la participación en el capital o en los derechos de voto correspondientes a acciones o participaciones es significativa cuando, por su proporción, permite a la persona que la posea tener capacidad de influencia en la persona jurídica participada.

Durante la tramitación del expediente, estas personas también 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.