CBNK

POLÍTICA DE GESTIÓN DE INFORMANTES

Versión 24 de junio de 2024

1. INTRODUCCIÓN

El objetivo de la presente Política de gestión de informantes (en adelante, la Política) es establecer el compromiso de Grupo CBNK, CBNK Banco de Colectivos, S.A como matriz y filiales, y la Dirección con un comportamiento y una cultura éticos en línea con los valores establecidos en nuestro Reglamento Interno de Conducta así como el compromiso para atender y gestionar de forma profesional y conforme a la normativa aplicable las comunicaciones de información que se reciban a través de los canales de información habilitados por la compañía, en relación con irregularidades o infracciones cometidas en el seno de la Entidad de acuerdo con el alcance definido en esta política.

La presente política se establece en cumplimiento 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 (en adelante, la Ley 2/2023). Esta ley transpone al ordenamiento jurídico español, la conocida como Directiva de "Whistleblowing", Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. En lo que se refiere a la normativa vigente en el ámbito nacional son diversos los ámbitos en los que ya se ha regulado la posibilidad de denuncias anónimas, a través del Real Decreto-ley 11/2018, de 31 de agosto, se introdujo en la ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, los procedimientos internos de comunicación de potenciales incumplimientos (canales de denuncias internas),y en otro ámbito, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la creación y mantenimiento de sistemas de información, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable, entre otras referencias normativas.

La Política se desarrolla y complementa con el Procedimiento de Gestión de Informantes de la Entidad y por el Reglamento Interno de Conducta (RIC).
Para elaborar la presente Política, se han tenido en cuenta las disposiciones de la Ley 2/2023.

2. PERSONAS SUJETAS

La presente Política es de aplicación a todos aquellos agentes que contribuyen a la actividad de la Entidad, que a los efectos del presente documento son:

- Empleados de la Entidad, con independencia de la modalidad contractual que determine su relación laboral, posición que ocupen o ámbito geográfico en el que desempeñen su trabajo.
- Socios y Directivos de la Entidad, con independencia de la modalidad contractual que determine su relación laboral o mercantil, posición que ocupen o ámbito geográfico en el que desempeñen su trabajo.
- Miembros del órgano de administración, sea cual sea la composición, forma y régimen de funcionamiento del órgano en cuestión de que se trate.

- Agentes que tengan un vínculo profesional con la Entidad (contratistas, partners, etc.)

(En adelante, las Personas Sujetas).

3. ÁMBITO DE APLICACIÓN

3.1. ¿QUIÉN PUEDE PRESENTAR UNA INFORMACIÓN?

De acuerdo con esta Política todos los integrantes de la Entidad, así como aquellos terceros no pertenecientes a la Entidad que hayan obtenido información sobre posibles irregularidades en un contexto laboral o profesional, podrán presentar comunicación de información por el canal habilitado, siempre que tengan un vínculo profesional o laboral con la Entidad. Por ejemplo, empleados, directivos, administradores, accionistas, autónomos, contratistas, subcontratistas, proveedores, etc.
Se incluyen, asimismo, aquellas personas que comuniquen información sobre infracciones obtenida en el marco de una relación laboral o estatutaria ya finalizada tales como, por ejemplo, voluntarios, becarios o trabajadores en formación, así como a aquellos cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.

A los efectos de este Procedimiento, las personas anteriormente indicadas que presenten una comunicación de información a través del canal de información de la Entidad se denominarán "informantes".

3.2. ALCANCE DEL CANAL DE INFORMANTES: ¿SOBRE QUÉ HECHOS SE PUEDE INFORMAR?

De acuerdo con esta Política, se puede enviar una comunicación para alertar de irregularidades, infracciones o incumplimientos en las siguientes materias:

- Todo comportamiento, acción o hecho que pueda constituir una violación de los códigos éticos y normas internas de Grupo CBNK, así como de las leyes y normativas que rigen la actividad del Grupo.
- Acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea siempre que entren dentro del ámbito de aplicación de los actos de la Unión Europea enumerados en el anexo de la Directiva UE (2019/1937); afecten a los intereses financieros de la UE; o incidan en el mercado interior en el sentido del artículo 2 de la Ley 2/2023.
- Acciones u omisiones que puedan constituir una infracción penal o administrativa grave o muy grave.

A los efectos de este Procedimiento, las conductas, acciones u omisiones anteriormente mencionadas se denominarán "irregularidades".
Las conductas que no contravengan lo anterior no deben tramitarse a través del Sistema, sino a través de otros cauces internos establecidos por la Entidad.

4. RESPONSABLE DEL SISTEMA INTERNO DE INFORMANTES

El órgano de administración/órgano de gobierno de la Entidad matriz, CBNK Banco de Colectivos, S.A, ha nombrado como Responsable del Sistema Interno de Informantes, al Comité de Ética y

Conducta y Unidad de Evaluación, delegando las facultades de gestión en la figura del Presidente del Comité, cuyos datos figuran en el anexo de esta Política (en adelante, el Responsable del Sistema).

El Responsable del Sistema es la persona en la cual se han delegado las facultades de gestión del Sistema interno de información y de tramitación de expedientes de investigación de la Entidad.

5. PROCESO DE GESTIÓN DE DENUNCIAS

5.1. CANAL INTERNO DE INFORMACIÓN

El canal interno de información facilitado por la Entidad se encuentra accesible a través del sitio web corporativo de la Entidad (www.cbnk.es), en la parte superior de la misma, en la sección denominada "Canal del Informante". También se puede acceder al canal a través de la siguiente dirección (en adelante denominado el Canal de Información):

https://www.cbnk.es/aviso-legal#canal-informante

El Canal de Información está basado en una herramienta proporcionada por Mazars Auditores, S.L.P. (Mazars) como proveedor externo de la Entidad, que se encarga de recibir y atender la comunicación de información recibida, con las debidas garantías legales de confidencialidad, seguridad y opción de anonimato previstas en la Ley.

Para presentar su comunicación de información, el informante accederá a la dirección arriba indicada donde la herramienta le informará de las vías a través de la cuales puede comunicar la información, las cuales son las siguientes:

- A través de la plataforma de Mazars cumplimentando el formulario correspondiente habilitado en la propia plataforma.
- A solicitud del informante, la comunicación también podrá presentarse mediante una reunión presencial dentro del plazo máximo de 7 días.

La comunicación de información puede transmitirse de forma anónima. El sistema otorga al informante un número de referencia para que pueda hacer seguimiento de su comunicación sin manifestar su identidad.

En caso de que el informante proporcione información sobre su identidad, ésta será tratada de manera confidencial y nunca se comunicará a la persona afectada/denunciada.

5.2. PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES

Recibida la comunicación de información por Mazars, como servicio externo e independiente a la Entidad, Mazars comunica al informante la recepción de la misma mediante acuse de recibo y le facilita un código de referencia a través de la plataforma, que permite la comunicación con el informante incluso aunque se trate de una comunicación anónima.

Tras un primer análisis preliminar de los hechos informados, Mazars contacta con el informante para ampliar o detallar la información en caso necesario y emite un Informe sobre la información recibida, sin identificar al informante.
El Informe de la comunicación recibida se remite al Responsable del Sistema interno de información de la Entidad, momento a partir del cual la comunicación es gestionada por el Responsable del Sistema.

El Responsable del Sistema, tras el análisis de los hechos informados, determina si los mismos forman parte o no del alcance del Canal de Información anteriormente indicado y procede a admitir/inadmitir la comunicación. En caso de admisión, se inicia la investigación de los hechos y tras su conclusión se determinan e implementan las medidas a adoptar por la Entidad.

5.3. PRINCIPIOS GENERALES DEL SISTEMA INTERNO DE INFORMACIÓN

Buena fe del informante

La buena fe, la conciencia honesta de que se han producido o pueden producirse hechos graves perjudiciales constituye un requisito indispensable para la protección del informante. Esa buena fe es la expresión de su comportamiento cívico y se contrapone a otras actuaciones que, por el contrario, resulta indispensable excluir de la protección, tales como la remisión de informaciones falsas o tergiversadas, así como aquellas que se han obtenido de manera ilícita.

Confidencialidad y preservación de la identidad del informante

La Entidad garantiza los principios de confidencialidad, seguridad y opción de anonimato en la gestión de las comunicaciones de información a través de un tercero externo e independiente que se encarga de la recepción de las informaciones.
Asimismo, la Entidad aplica las medidas técnicas, organizativas y de seguridad adecuadas para garantizar la protección de la información y cumple con la normativa de protección de datos personales.

Ausencia de represalias

La Entidad prohíbe expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación a través de los canales internos de denuncia. Entendiéndose por “represalia” cualesquiera actos u omisiones que estén prohibidos por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, solo por su condición de informantes, o por haber realizado una revelación pública.

5.4. DOCUMENTACIÓN Y PROTECCIÓN DE DATOS

De acuerdo con los requerimientos legales, las comunicaciones de información son registradas y documentadas en el Sistema interno de información, garantizando la confidencialidad y seguridad de la información, con acceso restringido exclusivamente al personal de la Entidad convenientemente autorizado y en cumplimiento de la normativa aplicable en materia de protección de datos personales.

En el momento en que el informante acceda al Canal se le informará de sus derechos de protección de datos a través de la correspondiente Política de Privacidad.

6. CANAL EXTERNO

Se pone de manifiesto la creación de un Canal externo de información gestionado por la Autoridad Independiente de Protección del Informante, A.A.I. que el informante podrá utilizar para presentar su comunicación de información, en el momento de su efectiva creación.

De esta forma, 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 incluidas en el ámbito de aplicación de la Ley 2/2023, ya sea directamente o previa comunicación a través del correspondiente canal interno.

De forma adicional, en materia de Prevención de Blanqueo de Capitales, los empleados, directivos y agentes que conozcan situaciones que puedan ser constitutivos de infracciones contempladas en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, los podrán poner en conocimiento del Servicio Ejecutivo de la Comisión (Sepblac).

7. APROBACIÓN

La presente Política de Gestión de Informantes ha sido aprobada por el órgano de administración de la Entidad y publicada por los instrumentos de comunicación interna de la Entidad. La Política se encuentra disponible en SharePoint, en la sección “Políticas y Procedimientos”.

Esta Política entrará en vigor al día siguiente de su publicación y se mantendrá en vigor hasta que sea actualizada o modificada por la siguiente versión, la cual será asimismo objeto de comunicación a los empleados y personas afectadas por esta Política.

Anexo: Datos del Responsable del Sistema

Responsable del Sistema interno de información:

Comité de Ética y Conducta y Unidad de Evaluación, delegando las facultades de gestión en la figura del Presidente del Comité, D. Eduardo Muela Rodríguez.