

## PROCEDIMIENTO DE GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN

De conformidad con la *Ley 2/2023*, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, así como con las políticas del *Grupo Mellenu* y los estándares internacionales aplicables, el presente procedimiento establece el marco de gestión del *Canal de Denuncias* de Vivus Financial Services S.A.U. El canal se configura como el medio habilitado para la comunicación segura y confidencial de infracciones o irregularidades administrativas, penales o de cualquier naturaleza vinculadas con la Entidad, velando por la adecuada recepción, análisis, tramitación y resolución de las comunicaciones recibidas en virtud de los principios de protección del informante, proporcionalidad, neutralidad y ausencia de represalias.

### Índice

1. Objeto y alcance .....	1
2. Responsables .....	1
3. Diagrama del procedimiento .....	1
4. Procedimiento de gestión .....	2
5. Procedimiento de gestión de la comunicación .....	3
5.1. Órgano receptor de las comunicaciones .....	3
5.2. Registro de las comunicaciones.....	3
5.3. Acuse de recibo e información al usuario sobre el Canal .....	3
6. Análisis de la comunicación y criterios de valoración .....	4
6.1. Comunicaciones desestimadas .....	4
6.2. Comunicaciones estimadas .....	4
7. Investigación, ejecución y cierre .....	4
8. Compromisos y principios.....	5
8.1. Medidas de protección y apoyo .....	6
8.2. Protección de datos personales.....	6
9. Aprobación y vigencia .....	7

## 1. Objeto y alcance

El presente documento tiene por objeto establecer y comunicar las pautas de gestión del Sistema Interno de Información, que incorpora el Canal de Denuncias como vía de comunicación segura respecto a irregularidades potenciales o ya ocurridas, relacionadas con Vivus Financial Services S.A.U. (en adelante, “**Vivus**” o “**la Entidad**”). El Canal de Denuncias es uno de los canales internos puestos a disposición por la Entidad como vía de recepción de comunicaciones respecto a hechos pasados, presentes o futuros dentro del alcance de algunos de los escenarios indicados a continuación:

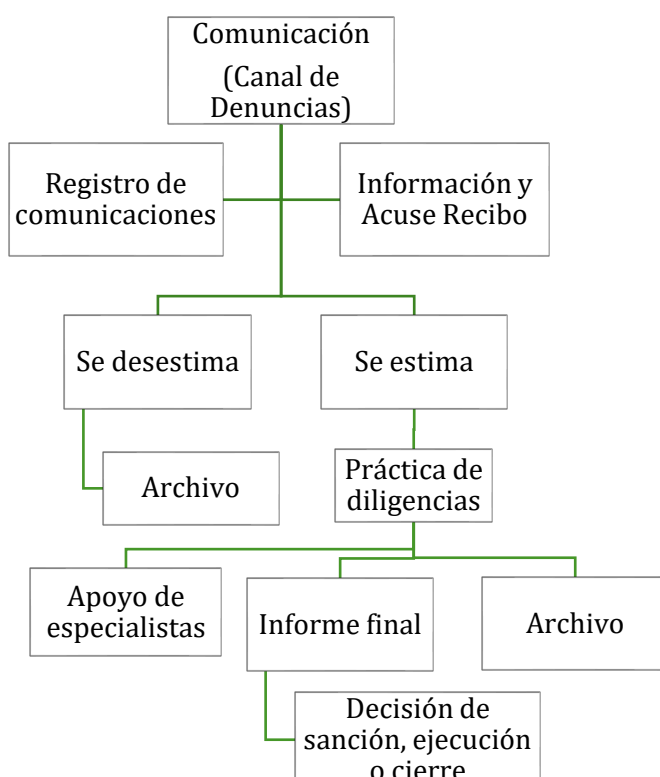
- Acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea siempre que estén dentro del ámbito de aplicación de los actos de la Unión Europea enumerados en el anexo de la Directiva (UE) 2019/1937, afecten a los intereses financieros de la Unión, o incidan en el mercado interior;
- Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave, incluyendo aquellas que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social;
- Acciones u omisiones que supongan incumplimientos éticos o de conducta.

Estos hechos podrán ser comunicados por toda persona física o jurídica (en adelante, “**Informante**”) que guarde o haya guardado relación con Vivus, que haya obtenido información sobre infracciones o irregularidades y lo comunique empleando el Canal de Denuncias o cualquier otra vía de comunicación interna establecida para los empleados y colaboradores de la Entidad.

## 2. Responsables

El Órgano de Control Interno (en adelante “**OCI**”) ha sido nombrado por el Órgano de Administración de Vivus como Órgano Colegiado responsable del Sistema Interno de Información de la Entidad, para la tramitación y gestión de las comunicaciones recibidas a través del Canal de Denuncias. A su vez, el OCI ha designado a un Responsable del Sistema Interno de Información (RSII) encargado de supervisar y garantizar su funcionamiento correcto. Las tareas relacionadas con la gestión del Sistema podrán ser divididas entre los miembros del OCI bajo la dirección de la persona a cargo de su presidencia. Los nombramientos y/o ceses dentro del órgano colegiado responsable del Sistema serán comunicados a la Autoridad Independiente de Protección del Informante en un plazo de 10 días hábiles, conforme al artículo 8 de la Ley 2/2023.

## 3. Diagrama del procedimiento



#### 4. Procedimiento de gestión

El enlace de acceso al Canal de Denuncias para el envío de comunicaciones por parte de los Informantes publicado en la página web de la Entidad, que se difunde a los empleados mediante las formaciones internas y que además se encuentra en distintos espacios físicos de la sede de la Compañía, es el siguiente: <https://app.falcony.io/wb4finance/links/whistleblowing>

Si por algún motivo no fuese posible la comunicación mediante el enlace indicado, la comunicación podrá remitirse por correo postal dirigida al Órgano de Control Interno:

ÓRGANO DE CONTROL INTERNO

Vivus Financial Services S.A.U.

C. de Albasanz, 14, 28037, Madrid.

Adicionalmente, los empleados de Vivus podrán formular sus comunicaciones por cualquier medio ante su superior jerárquico, quien deberá comunicarse con el OCI para su adecuada gestión. De igual forma, a solicitud del Informante, la comunicación también se podrá presentar ante el OCI mediante una reunión presencial dentro del plazo máximo de 7 días. En caso de que estas comunicaciones verbales sean grabadas o transcritas, se solicitará al Informante, de forma clara y previa, su consentimiento para la grabación o transcripción de estas, y se le ofrecerá la oportunidad de comprobar, rectificar y aceptar el texto transcrito o audio grabado.

El Órgano de Control Interno, como encargado de gestionar el Sistema Interno de Información, no revelará en ningún momento la identidad del Informante de buena fe, salvo requerimiento judicial u obligación legal. Vivus ha adoptado las medidas necesarias para garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente de la persona que hubiera puesto los hechos en conocimiento de la entidad.

Las comunicaciones podrán ser anónimas si así lo desea el Informante, sin perjuicio de la valoración que pueda realizarse de las mismas conforme a los criterios que se expondrán en este Procedimiento, los Informantes deciden si sus comunicaciones serán anónimas o no durante el proceso de formulación de sus comunicaciones. Si la comunicación no fuera anónima, deberá contener el nombre del Informante y los datos de contacto: teléfono y dirección de correo electrónico, a efectos de seguimiento y notificaciones. Si la comunicación fuera anónima o no lo fuera, de igual manera deberá incluir lo siguiente:

- Contenido de la comunicación: deberán describirse de manera concreta y precisa los hechos sucedidos, la sociedad y el área afectada, la fecha o periodo de comisión y los posibles sujetos responsables;
- Las comunicaciones deberán acompañarse de toda la información relevante, en cualquier soporte (documento, audio, vídeo) que se encuentre a disposición del Informante.

Cabe destacar que el Informante también puede acceder a los canales externos de información ante las autoridades nacionales o autonómicas y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea, cuya gestión estará sujeta a los criterios de dichas autoridades. A continuación, se citan algunos de los Canales Externos de Información para la comunicación de irregularidades previstas en la Ley 2/2023:

- En el supuesto de infracciones del derecho de la Unión Europea graves o muy graves que afecten al ámbito estatal en materia de transparencia y buen gobierno, podrá optarse por los cauces previstos ante la Autoridad Independiente de Protección del Informante, que pueden consultarse en [este enlace](#);
- En caso de infracciones que afecten al ámbito autonómico, se podrá recurrir a los canales previstos por el Consejo de Transparencia y Protección de Datos de la comunidad de Madrid, que se pueden consultar en [este enlace](#);

- Respecto a servicios, productos, prevención del blanqueo de capitales y la financiación del terrorismo, se citan los siguientes enlaces para las comunicaciones:
  - [SEPBLAC](#);
  - [Banco de España](#);
  - [Comisión Nacional del Mercado de Valores](#).
- En caso de infracciones administrativas contra la competencia, además, se puede optar por el canal externo de la Comisión Nacional de los Mercados y la Competencia (CNMC), accesible a través de [este enlace](#);
- Otros Canales Externos de Información y Autonómicos citados por la Autoridad Independiente de Protección del Informante pueden consultarse pinchando [aquí](#).

## 5. Procedimiento de gestión de la comunicación

### 5.1. Órgano receptor de las comunicaciones

Las comunicaciones formuladas a través del Canal de Denuncias serán recibidas por el Responsable del Sistema Interno de Información, que, forma parte del Órgano de Control Interno de la Entidad. Este órgano es responsable por el cumplimiento del presente procedimiento de gestión sin perjuicio de la delegación de las funciones de gestión e investigación que se pudieran realizar. El proceso de gestión de las comunicaciones tendrá un plazo no superior al plazo máximo de 3 meses, en cumplimiento del [artículo 9](#) de la Ley 2/2023 sobre el procedimiento de gestión de informaciones, no obstante, este plazo podrá extenderse otros 3 meses adicionales en casos de especial complejidad.

En el supuesto de que la comunicación recibida se refiera a alguno de los responsables del canal o se detecte un posible conflicto de intereses, este se abstendrá de intervenir en cualquier fase de los procedimientos y comunicará esta circunstancia de manera inmediata a la Dirección de la Entidad. En caso de que el hecho comunicado por el Informante presente indicios de una acción constitutiva de delito, se remitirá la información recibida con carácter inmediato al Ministerio Fiscal, salvo que los hechos afecten los intereses financieros de la Unión Europea, en cuyo caso se remitirá a la Fiscalía Europea.

### 5.2. Registro de las comunicaciones

Todas las comunicaciones recibidas serán registradas por la Entidad de carácter no público con fines de control, seguimiento y auditoría. Como mínimo, se incluirán los siguientes campos:

- Número de referencia.
- Fecha de recepción.
- Descripción de la comunicación.
- Medidas adoptadas.
- Fecha de cierre.

### 5.3. Acuse de recibo e información al usuario sobre el Canal

Con el fin de que el Informante pueda constatar la recepción de la comunicación, el acuse de recibo se emitirá en un plazo máximo de 7 días. Respecto a la información a disposición de los Informantes, en el mismo canal y en su [Política de Privacidad](#) se destacan sus características en cumplimiento de la normativa aplicable:

- Anonimato por defecto a menos que el Informante decida identificarse;
- Periodo de conservación de datos;
- Responsables del tratamiento de datos;
- Canales de consulta sobre datos personales y base legal del Canal de Denuncias.

## 6. Análisis de la comunicación y criterios de valoración

Las comunicaciones recibidas a través del Canal de Denuncias serán analizadas para valorar si el hecho comunicado pudiera ser considerado como irregularidad o infracción de acuerdo con el artículo 2 del ámbito de aplicación de la Ley 2/2023 y valorar si se vulnerara alguna de las políticas o códigos éticos del Grupo Mellenu o de Vivus. Además, se evaluará si la comunicación presentada resulta verosímil y fuera realizada de buena fe, o si, por el contrario, pudiera haberse formulado de forma intencionadamente falsa o de mala fe, las cuales serán comunicadas a la Dirección de la Entidad y estarán sujetas a medidas disciplinarias.

Se considera que el Informante actúa de buena fe cuando su comunicación esté basada en hechos o indicios de los que razonablemente pueda identificarse alguna irregularidad. Las comunicaciones deberán realizarse sin dolo, mala fe y sin ánimo de perjudicar a la Entidad o al Grupo.

### 6.1. Comunicaciones desestimadas

Las comunicaciones desestimadas serán registradas de igual manera en la herramienta de gestión de las comunicaciones, incluyendo la información relativa a la fecha y motivo de cierre y se archivarán de forma anonimizada. En todo caso, las siguientes comunicaciones no serán admitidas a trámite:

- Comunicaciones que no se refieran a hechos que puedan constituir una infracción de cualquier normativa o ilícito penal, incluida la normativa interna del Grupo Mellenu;
- Comunicaciones con información incompleta, inconsistente o con imprecisiones manifiestas;
- Comunicaciones que aparezcan como manifiestamente infundadas o inverosímiles.

### 6.2. Comunicaciones estimadas

Las comunicaciones estimadas serán gestionadas en un plazo inferior a 3 meses, incluyendo la información relativa a la fecha y al motivo de cierre, este periodo podrá extenderse según el nivel necesario de investigación, preservación y custodia de evidencias antes del cierre, lo cual será comunicado al Informante. En caso de ser necesario, se mantendrá comunicación con el Informante, con la posibilidad de solicitarle información adicional, para así obtener información suplementaria que pueda ayudar al esclarecimiento de los hechos.

Cuando se requieran datos personales a cualquiera de las partes intervinientes en el proceso, se informará de forma expresa que los datos recogidos en la presente investigación serán tratados por la organización como Responsable del tratamiento.

## 7. Investigación, ejecución y cierre

Tras la admisión de la comunicación, el Responsable del Canal llevará a cabo las debidas diligencias para los esclarecimientos necesarios y podrá solicitar el apoyo de especialistas según la complejidad de las investigaciones, que, deberán cumplir con las normativas de protección de datos y de derechos laborales -citado de manera enunciativa y no limitativa-, además de los principios presentes en este procedimiento. Dichas diligencias que serán debidamente documentadas, a modo de ejemplo, podrán consistir en:

- Entrevistas con el investigado o con otras personas;
- Solicitudes de información y documentación al investigado o a terceros;
- Recabar información o documentación de Vivus o del Grupo Mellenu;
- Solicitar el apoyo de investigadores o consultores externos;
- Cualquier otra diligencia considerada necesaria para llevar a cabo la investigación.

El contenido del Informe Final incluirá mínimamente las siguientes informaciones:

- Propuesta de sanción o archivo, debidamente justificado;
- Diligencias practicadas y conclusiones obtenidas;
- Infracciones o irregularidades identificadas;
- Propuesta de medidas disciplinarias respecto al responsable o responsables;
- Alegaciones del investigado, con un plazo otorgado no inferior a 10 días hábiles, la presentación de sus alegaciones y pruebas que considere oportunas.

En caso de propuesta de sanción, el informe será emitido a la Dirección de Vivus, que será responsable por la ejecución de las medidas oportunas. Una vez aplicadas estas medidas, la comunicación será archivada y registrada junto con todas las informaciones correspondientes, velando por la trazabilidad adecuada del proceso.

## 8. Compromisos y principios

En cumplimiento de las medidas de protección respecto a los Informantes y a todas las personas a las que se refieran las comunicaciones recibidas mediante el Canal de Denuncias, el presente procedimiento se basa, entre otros, en los siguientes principios:

- Transparencia;
- Confidencialidad;
- Presunción de inocencia;
- Protección frente a represalias de conformidad con las [medidas de protección](#) establecidas por la Ley 2/2023.

Se velará por la confidencialidad absoluta del contenido de las comunicaciones y la identidad de las personas involucradas ante terceros, incluyendo empleados o representantes de Vivus, a excepción de que deban ponerse a disposición de las autoridades competentes según el resultado de las investigaciones. Las comunicaciones de forma verbal (incluyendo reuniones presenciales) serán documentadas, previo consentimiento del Informante, mediante su grabación o transcripción en un formato seguro, duradero y accesible, para su posterior comprobación, rectificación y aceptación por parte del Informante.

No será aplicable ningún tipo de represalia o consecuencia negativa contra el Informante, salvo que la investigación interna determine que la comunicación ha sido realizada con conocimiento de su falsedad o que se ha realizado con temerario desprecio hacia la verdad, mala fe o abuso de derecho, este tipo de comunicaciones constituyen una infracción grave de las políticas de la Entidad y del Grupo y podrá dar lugar a las correspondientes sanciones disciplinarias. Los Informantes que hayan participado en la infracción de las políticas del Grupo Mellenu no resultarán exentos de su eventual responsabilidad por el mero hecho de haber formulado la comunicación.

Las personas investigadas deberán colaborar cuando sea requerido, para que la Entidad pueda llevar a cabo las diligencias debidas durante el transcurso de la investigación de las comunicaciones recibidas por los Informantes y podrán requerir asistencia legal. Tanto la identidad como el contenido de la investigación (hechos investigados, tramitación, diligencias practicadas, informe resultante y decisión) están amparados bajo los principios y normativas aplicables al presente procedimiento, incluyendo el derecho a la presunción de inocencia, acceso al expediente y defensa. En cualquier momento durante el desarrollo de la investigación, el investigado o las personas reflejadas en el alcance del presente procedimiento deberán (i) exponer su versión completa de los hechos, sea verbalmente o por escrito, y (ii) aportar a la investigación cuantos documentos o testimonios consideren oportunos o sean requeridos para el esclarecimiento de los hechos.

El investigado será informado de las decisiones que pueda adoptar la Entidad como resultado de la investigación y deberá mantener la confidencialidad acerca de la existencia de la investigación y de su contenido. En caso de incumplimiento de las obligaciones descritas anteriormente por parte del investigado, podrá aplicársele la sanción disciplinaria conforme a la normativa laboral vigente a criterio de la Dirección. El mero hecho de ser una persona colaboradora no investigada no será criterio para sanción o represalia alguna.

## 8.1. Medidas de protección y apoyo

Las personas que comuniquen infracciones conforme al artículo 2 de la Ley 2/2023 podrán acogerse a las medidas de protección establecidas en el Título VII (artículos 35 a 39) siempre que existan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación o revelación, aun cuando no se aporten pruebas concluyentes y cuando la comunicación se haya realizado conforme a los requerimientos previstos en la ley. Se incluyen además las comunicaciones públicas anónimas, pero que de forma posterior hubieran sido identificadas y cumplan con las condiciones establecidas en la ley, además de las informaciones realizadas ante las instituciones, órganos u organismos pertinentes de la Unión Europea, infracciones que entren en el ámbito de aplicación de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019.

De las medidas de protección previstas por la normativa quedan excluidas las personas que hayan comunicado informaciones inadmitidas, reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación, las informaciones disponibles para el público o aquellas que pudieran considerarse rumores y las informaciones no comprendidas en el ámbito de material de aplicación de la ley (artículo 2).

Las medidas de protección del Informante también se aplicarán a los representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al Informante; a las personas físicas, que, en el marco de la organización en la que preste servicios el Informante, asistan al mismo en el proceso; a las personas físicas que estén relacionadas con el Informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del Informante; a 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.

## 8.2. Protección de datos personales

El Sistema Interno de Información de la Entidad y su procedimiento de gestión han sido implementados de conformidad con el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018 de Protección de Datos y Garantía de los Derechos digitales. En calidad de responsables del tratamiento de forma conjunta, Vivus Financial Services S.A.U. y el Grupo Mellenu, tratarán los datos personales respecto a las comunicaciones recibidas únicamente para la gestión de estas siguiendo los principios establecidos por el marco normativo de protección de datos.

Los titulares de los datos personales relacionados con las comunicaciones recibidas podrán ejercitar sus derechos de protección de datos -acceso, rectificación, supresión y oposición- según lo dispuesto en la normativa aplicable de protección de datos personales mediante el envío de un correo electrónico a la dirección: [dpd@vivus.es](mailto:dpd@vivus.es). El ejercicio de tales derechos no implicará la revelación de información confidencial o los datos identificativos del Informante o demás partes involucradas.

Los datos personales objeto de tratamiento serán conservados en el Sistema Interno de Información únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos comunicados, se procederá a la supresión de datos personales que no sean necesarios para el curso de la investigación y que no tuvieran relación con las comunicaciones previstas en la Ley 2/2023. En todo caso, transcurridos 3 meses desde la recepción de la comunicación en el Sistema Interno sin haber iniciado actuaciones de investigación, deberá procederse a su supresión del Sistema, salvo que la finalidad de la conservación sea para evidenciar el funcionamiento del Sistema, en cuyo caso, las comunicaciones a las que no se haya dado curso constarán de forma anonimizada. Transcurridos los plazos citados, los datos podrán seguir siendo tratados por los órganos a los que corresponda, para dar continuidad a la investigación de las infracciones comunicadas, no conservándose la información en el Sistema Interno de Información de la Entidad.

Conforme al artículo 32 de la Ley 2/2023, el acceso a los datos personales contenidos en el Sistema Interno de Información está delimitado a:

- El Responsable del Sistema Interno de Información en representación del Órgano de Control Interno;
- El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador;
- El responsable de los servicios jurídicos de la Entidad y del Grupo, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación;
- Los encargados del tratamiento, que eventualmente sean designados;
- El Delegado de Protección de Datos.

Finalmente, para un uso adecuado del Canal de Denuncias como Sistema Interno de Información de la Entidad, el presente procedimiento, puesto a disposición de las partes interesadas, no exime del conocimiento y lectura 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, así como de su marco normativo aplicable. Se recomienda la lectura y conocimiento de dicha normativa para una correcta comprensión y utilización del Canal de Denuncias.

### 9. Aprobación y vigencia

Aprobado por	Efectivo desde
Órgano de Control Interno	Junio, 2026