PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES

SISTEMA INTERNO DE INFORMACIÓN DE VIRTON S.A.

Autor	Revisado por	Aprobado por
Responsable del Sistema interno de información	Director Gerente	Consejo de Administración
Fecha: 04/04/2025	Fecha: 04/04/2025	Fecha: 07/04/2025

ÍNDICE

1. Introducción

Objetivos del Procedimiento

El Procedimiento de Gestión de Informaciones (en adelante, el "**Procedimiento**") tiene como finalidad que el personal de Empresa de VIRTON, S.A., así como sus partes interesadas, dispongan de una información clara y fácilmente accesible sobre el **funcionamiento y actuaciones a seguir para el uso del canal interno de información de VIRTON, S.A.**, así como sus **garantías de protección frente a posibles represalias[1] comunicando infracciones**, en base a lo dispuesto en 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" o la "Ley").

Adicionalmente, el presente Procedimiento tiene las siguientes finalidades en relación con el personal a la hora de informar sobre infracciones:

- ✓ Animarles a sentirse **cómodos y seguros**;
- ✓ Proporcionarles **vías para informar de forma confidencial o anónima**, y recibir información sobre las medidas adoptadas;
- ✓ Garantizar que **reciban una respuesta**, siempre que sea posible, a la información revelada.

Asimismo, este procedimiento detallará, entre otros:

- ✓ Las **responsabilidades de implantación y de gestión del Sistema interno de información**
- ✓ La identificación y descripción de las **distintas formas de comunicación permitidas por el canal interno de información**
- ✓ La identificación y descripción del **canal externo de información** de la Autoridad Independiente de Protección del Informante
- ✓ La **protección de datos** personales
- ✓ Las **definiciones[2] más relevantes** para entender mejor este procedimiento y la Ley 2/2023

El Procedimiento está **alineado con el Código Ético de VIRTON, S.A.**, que establece los valores de la Sociedad, y, por tanto, deben leerse y entenderse ambos documentos de manera conjunta.

[1] Anexo 1: Ley 2/2023, de 20 de febrero, art. 36 "Prohibición de represalias"
[2] Anexo 2: Definiciones

¿A qué tipo de comunicaciones se aplica?

El ámbito material de aplicación[3] de la Ley 2/2023 comprende todas las comunicaciones que traten sobre:

- ✓ **Infracciones del Derecho de la Unión Europea** cuando:
  - Afecten a alguna de las materias señaladas en el **ámbito de aplicación del artículo 2[4] de la Directiva (UE) 2019/1937** del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, o **Directiva Whistleblowing.**
  - Afecten a los intereses financieros de la Unión, o
  - Incidan en el mercado interior;
- ✓ **Infracciones administrativas graves o muy graves**, o
- ✓ **Hechos delictivos**.

¿A quién protege la Ley?

A **cualquier persona** que en un **contexto laboral o profesional** haya obtenido información sobre presuntas infracciones, ya sea en el sector público o en el privado. La protección no se circunscribe a los empleados de los sujetos obligados, sino también a cualquier otra persona que, en el ejercicio profesional o en el marco de la prestación de servicios, haya interactuado con dichos sujetos. La Ley 2/2023 incluye el siguiente listado no exhaustivo[5]:

- ✓ Empleados públicos
- ✓ Trabajadores por cuenta ajena
- ✓ Autónomos
- ✓ Accionistas, miembros del órgano de administración, dirección o supervisión
- ✓ Voluntarios, becarios y trabajadores en períodos de formación; y
- ✓ Cualquier persona que trabaje para contratistas, subcontratistas y proveedores.

Las comunicaciones pueden referirse a **presuntas infracciones en el ámbito de una relación laboral o profesional todavía en vigor, ya finalizada o incluso no iniciada** (por ejemplo, si se refiere a infracciones relativas a procesos de selección o de negociación precontractual).

El **alcance de la protección se extiende a las personas relacionadas con el informante** (compañeros de trabajo, familiares, personas jurídicas para las que trabaje o de las que sea titular, etc.). Asimismo, se extenderá a **toda persona física que haya asistido al informante** y,

[3] Anexo 2: Definiciones ("Ámbito material de aplicación")
[4] Anexo 3: Directiva (UE) 2019/1937, art.2 "Ámbito de aplicación material"
[5] Anexo 2: Definiciones ("Ámbito personal de aplicación")

específicamente, a los representantes legales de los trabajadores en el ejercicio de sus funciones de asesoramiento y apoyo al informante.

2. Responsabilidades acerca del Sistema interno de información

Consejo de Administración

El **Consejo de Administración** es el **responsable de la implantación del Sistema interno de información**, previa consulta con la representación legal de las personas trabajadoras, y tendrá la **condición de responsable del tratamiento de los datos personales** de conformidad con lo dispuesto en la normativa sobre protección de datos personales.

Responsable del Sistema interno de información

El Consejo de Administración ha designado al **Manuel Carrillo** de VIRTON, S.A., como la **persona física responsable de la gestión de dicho sistema** o "**Responsable del Sistema interno de información**" (en adelante, "**Responsable del Sistema**"). El Consejo de Administración será igualmente responsable del cese del Responsable del Sistema.

Tanto el nombramiento como el cese de la persona física individualmente designada, **deberá ser notificado a la Autoridad Independiente de Protección del Informante**, o, en su caso, a las **autoridades u órganos competentes de las comunidades autónomas,** en el ámbito de sus respectivas competencias, **en el plazo de los diez días hábiles siguientes**, especificando, en el caso de su cese, las razones que han justificado el mismo.

El **Responsable del Sistema desarrollará sus funciones de forma independiente y autónoma respecto del resto de los órganos** de la Sociedad (la Junta General, el Consejo de Administración y la Gerencia), y **no podrá recibir instrucciones de ningún tipo en su ejercicio**, y deberá **disponer de todos los medios personales y materiales necesarios para llevarlas a cabo**.

3. Canal interno de información

En línea con el compromiso de VIRTON, S.A., con el principio de integridad y la necesidad de actuar éticamente, todo el personal, así como las partes interesadas, deben **poder comunicar infracciones o presuntos incumplimientos**, al tener **conocimiento de los mismos o detectar indicios razonables** de su comisión en la Sociedad.

Las **comunicaciones de infracciones que queden fuera del ámbito de aplicación material de la Ley 2/2023** (ir al apartado de "Definiciones", y/o art. 2 de la Ley), **y sus remitentes, quedarán fuera del ámbito de protección dispensado por la organización en virtud de la misma**.

VIRTON S.A., **investigará todas las comunicaciones**, siempre y cuando el uso de las **distintas formas de comunicación del canal interno de información**, se haga cumpliendo con las siguientes **condiciones**:

- ✓ Se utilizará sólo para los **fines para los que ha sido creado**. No se investigarán la presentación de quejas personales, diferencias o conflictos personales, etc.
- ✓ Las comunicaciones deben estar basadas en la **buena fe y en el ofrecimiento de un contenido veraz**: no falta a la buena fe quien comunica una irregularidad que finalmente resulta no serlo o no puede ser debidamente probada. Sí falta a la buena fe quien comunica hechos que sabe que no son ciertos con el fin de perjudicar a otras personas o a la propia Sociedad.

Aquellas comunicaciones que no guarden una clara relación con dicho compromiso (deliberadamente falsas o de mala fe serán sujetas a la adopción de posibles **medidas disciplinarias** e incluso a la interposición de **demandas legales**.

Acceso a las distintas vías de comunicación del Canal interno de información

El **canal interno de información** de VIRTON, S.A., permite realizar **comunicaciones por escrito o verbalmente**, o de las dos formas:

- ✓ Por escrito:
  - A través del siguiente **correo electrónico**: canal-etico@virton.es
- ✓ Verbalmente: a través de un **sistema de mensajería de voz**
- ✓ Presencialmente: el informante podrá solicitar una **reunión presencial**, poniéndolo en conocimiento del Responsable del Sistema interno de información, que deberá convocarla dentro del **plazo máximo de siete (7) días** desde su solicitud.

Las comunicaciones verbales, es decir, las realizadas a través de reunión presencial o mediante sistema de mensajería de voz, **se documentarán de alguna de las siguientes maneras, previo consentimiento del informante**:

- ✓ Mediante una **grabación de la conversación** en un formato seguro, duradero y accesible, o;
- ✓ A través de una **transcripción completa y exacta de la conversación** realizada por el personal responsable de tratarla. Sin perjuicio de los derechos que le corresponden de acuerdo a la normativa sobre protección de datos, **se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación**.

Asimismo, **en cumplimiento** del:

- ✓ *Art. 5.2.d) de la Ley "El **Sistema interno de información**, en cualquiera de sus fórmulas de gestión, **deberá integrar los distintos canales internos de información que pudieran establecerse dentro de la entidad**.",*

Garantías de confidencialidad y anonimato

Las **distintas formas de comunicación** permitidas por el **canal interno de información** de VIRTON, S.A., están diseñadas y gestionadas de una forma segura, de modo que se **garantizan la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación**, y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la **protección de datos, impidiendo el acceso de personal no autorizado**.

VIRTON, S.A., **garantiza igualmente la confidencialidad** cuando la comunicación sea remitida a miembros del personal no responsable de su tratamiento (responsable jerárquico, un miembro del departamento de Recursos Humanos, etc.) quienes tienen la **obligación de remitirla inmediatamente al Responsable del Sistema**.

Por último, el **Canal Ético de VIRTON, S.A., permite** la presentación y posterior **tramitación de comunicaciones anónimas**.

¿Cómo se gestionarán las comunicaciones?

El **Responsable del Sistema** será el **encargado** de **la recepción y gestión completa de las comunicaciones** realizadas por cualquiera de las posibles vías indicadas anteriormente:

Recepción y evaluación de la comunicación

- ✓ Si, tras una **evaluación preliminar**, el Responsable del sistema llega a la conclusión de que la comunicación es **pertinente y existen motivos reales de preocupación**, iniciará una investigación que se realizará de forma justa y objetiva.

  Por su parte, si, tras la evaluación inicial, considera la comunicación **no pertinente e improcedente** porque **no hay pruebas suficientes** de que se haya cometido una infracción, o porque **no está relacionada con las materias** a comunicar a través del canal, se informará al informante (siempre que no haya sido una comunicación anónima a través de la mensajería de voz) y se archivará la comunicación.

- ✓ Envío de **acuse de recibo** de la comunicación al informante, en el plazo de **siete días naturales** siguientes a su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.

  En caso de que el informante realice una comunicación a través del **Canal Ético**, le aparecerá en el portal una **confirmación de manera inmediata de la correcta creación de la misma**, sea confidencial o anónima. Si fuese **anónima**, en esta misma confirmación, se le proporcionará un **código único que le permitirá conocer en cada momento el estado de su comunicación** (pero en ningún caso le permitirá mantener la comunicación o facilitar información adicional al Responsable del Sistema).

- ✓ El Responsable del Sistema **remitirá la comunicación al Ministerio Fiscal con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito**. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

Investigación de la comunicación

- ✓ El **plazo máximo para dar respuesta a las actuaciones de investigación no podrá ser superior a tres meses** a contar desde la recepción de la comunicación o, si no se remitió 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 del plazo, en cuyo caso, este podrá extenderse **hasta un máximo de otros tres meses adicionales**.

- ✓ Durante el proceso de investigación el Responsable del Sistema podrá **consultar al Jefe de Sección de Recursos Humanos**, a fin de tratar las implicaciones en materia laboral o legal que pudieran conllevar los hechos comunicados.

- ✓ Previsión de la **posibilidad de mantener la comunicación con el informante** y, si se considera necesario, de solicitar a la persona informante información adicional (siempre que no haya sido una comunicación anónima a través de la mensajería de voz o del Canal Ético).

- ✓ Establecimiento del **derecho de la persona afectada a que se le informe de las acciones u omisiones que se le atribuyen**, y a ser oída en cualquier momento. Dicha comunicación

tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.

En ningún caso se permitirá a la persona afectada **conocer la identidad del informante**, ni el contenido completo de la comunicación o cualquier otra información que **pudiera revelar la identidad del mismo**.

Resolución, cierre y respuesta

Una vez recabadas las **pruebas pertinentes**, y analizadas junto con toda la información disponible desde el inicio de la comunicación, el Responsable del Sistema **trasladará el informe de conclusiones de la investigación al "Órgano de Decisión"** para que adopte las medidas más oportunas y cierre la investigación. Dicho órgano estará **compuesto por tres miembros y tendrá la naturaleza de órgano mixto, con autoridad suficiente** para tomar decisiones en nombre de VIRTON S.A..

Las infracciones serán sancionadas a través del **régimen sancionador del convenio colectivo** al que VIERON, S.A., se encuentra adherido.

Finalmente, se comunicará a las partes implicadas la resolución adoptada.

Derecho a la presunción de inocencia y a la defensa de las personas afectadas

Durante la tramitación de la investigación las personas afectadas por la comunicación tendrán **derecho a la presunción de inocencia**, al **derecho de defensa** y al **derecho de acceso al expediente** en los términos regulados en la 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.

4. Canal externo de información

Se regula en la Directiva 2019/1937 un canal externo de información presidida por los principios de independencia y autonomía en la recepción y tratamiento de la información sobre las infracciones.

El canal interno de información debe ser complementado con un canal externo, es decir, los informantes tienen la posibilidad de, alternativamente, remitir su comunicación directamente, o con posterioridad al envío de la comunicación a través del canal interno de información de VIRTON, S.A., ante las autoridades públicas por medio del **canal externo de comunicación habilitado por la Autoridad Independiente de Protección del Informante**, de acuerdo con los términos establecidos en el Título III de la Ley:

- ✓ *"Art. 16 de la Ley: **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 esta ley**, ya sea directamente o previa comunicación a través del correspondiente canal interno."*.

En el caso de **VIRTON, S.A.,** la autoridad autonómica competente como canal externo de información es el **Canal del Informante**, un canal que permite comunicar las posibles infracciones del ordenamiento jurídico, y que tiene su antecedente en la Directiva UE 2019/1937, y Decreto 63/2022 del 20 de julio. Además del Canal del Informante, existen otros canales para comunicar información sobre posibles infracciones del ordenamiento jurídico por motivo de su actividad en el ámbito de la Administración autonómica, es decir, canales estatales o europeos. Además, disponemos de otros canales externos a nivel estatal como *Servicio Nacional de Coordinación Antifraude* o la *Fiscalía contra la Corrupción y la Criminalidad Organizada*. Concretamente nos interesa este último donde encontramos la fiscalía de la Comunidad de Madrid que obedece en todo el territorio de la Comunidad Autónoma.

Creación

Siguiendo el informe de la Comisión Europea de 3 de febrero de 2014, se crea el Canal de Denuncias de la Oficina Municipal contra el Fraude y la Corrupción (en adelante la "**Oficina**") o el Canal del Informante, que hemos introducido en el apartado anterior. Dichos canales se configuran como los canales externos **de información previsto en el artículo 16 de la Ley 2/2023** (en adelante, "**Canal externo**").

Anonimato y confidencialidad

El canal externo **admite comunicaciones anónimas**, y el informante que opte por identificarse podrá solicitar de la Oficina que se guarde la confidencialidad sobre su identidad, así como

respecto de cualquier otra información de la que ésta se pueda deducir, directa o indirectamente; estando el personal de la Oficina obligado a mantenerla, aun cuando la persona afectada solicite conocer la identidad del informante.

El Canal del Informante también permite la **Anonimización de datos personales**. En este caso se garantiza la confidencialidad de la identidad mediante algoritmos de encriptación desde el envío hasta la finalización de los trámites que correspondan.

Acceso al canal externo

En lo referente al Canal del Informante, se habilita el mismo en el portal web de la institución Canal del Informante | Portal de Transparencia (comunidad.madrid). En este caso, la comunicación de información se puede realizar a través de los siguientes medios:

- ✓ Presentación on line con certificado electrónico.
- ✓ Presentación on line sin certificado electrónico.
- ✓ Presentación verbal de información mediante comparecencia personal.

En el caso de utilizar la *Fiscalía contra la Corrupción y la Criminalidad Organizada*, podemos acudir a la web Home - Fiscal.es. En cuyo caso disponemos de un email fiscaliacm@madrid.org, un teléfono de contacto y una dirección. Además, hay una pestaña sobre "áreas especializadas" donde podremos ponernos en contacto directamente rellenando unos parámetros.

Titularidad y gestión del canal externo

- ✓ La **titularidad** del canal externo, del portal web y del dominio en internet corresponde a la Oficina. En cuanto al Canal del Informante, a la propia Comunidad de Madrid.
- ✓ Su **mantenimiento** y evolución tecnológica corresponde a la Oficina. En cuanto al Canal del Informante, a la propia Comunidad de Madrid.
- ✓ La **gestión de sus contenidos y funcionalidades** corresponde a la subdirección de la Oficina competente en materia de protección del denunciante y gestión del canal de denuncias, conforme a lo previsto en el artículo 23 y 24 del Reglamento Orgánico de la Oficina Municipal de Madrid contra el Fraude y la Corrupción (BOCM Nº11, del 13 de enero de 2017) respecto del tratamiento de la información y reserva de identidad. En el caso del Canal del Informante, le corresponde tramitar las comunicaciones de información presentadas a través del Canal a los centros directivos con competencia en materia de inspección de la Comunidad de Madrid, así como a aquellos órganos o unidades que, por razón de la materia, puedan ponerse en funcionamiento para el conocimiento de informaciones sobre posibles infracciones en sus correspondientes ámbitos.

Contenidos y servicios del canal externo

El canal externo de la Oficina dispone de los siguientes contenidos y servicios:

- ✓ **Comunicación con solicitud de medida de protección**: en este caso, el informante deberá identificarse con sus datos personales de contacto.
- ✓ **Comunicación sin solicitud de medida de protección**: en este caso, el informante podrá optar por identificarse o por presentar una denuncia anónima.
- ✓ **Seguimiento de denuncias**: permitirá al informante consultar el estado de tramitación de una comunicación o aportar más información sobre una comunicación ya presentada, incluso en el caso de haber presentado la comunicación de forma anónima, ya que se facilitará a toda comunicación presentada un código numérico único para el acceso o seguimiento posterior.

En el caso del Canal del Informante, dispone de los siguientes servicios:

- ✓ **Anonimización de los datos personales**: se garantiza la confidencialidad y la identidad mediante algoritmos de encriptación, desde el envío de la comunicación hasta la finalización de los trámites.
- ✓ **Notificaciones**: si la comunicación se realiza sin la Anonimización de los datos personales, las notificaciones se realizarán por medios electrónicos a través del Sistema de Notificaciones Electrónicas de la Comunidad de Madrid. Si la comunicación se hace a través de la Anonimización de los datos personales, las comunicaciones que envíe la unidad de tramitación lo hará por correo electrónico garantizando el anonimato de la identidad.
- ✓ **Consulta del expediente y envío de información**: para la consulta de situación del expediente y aportar documentos y enviar comunicaciones.
- ✓ **Otros canales externos**: ponen a disposición otros canales externos para aquellos que tengan información sobre posibles infracciones del ordenamiento jurídico:
    - Canales estatales: Servicio Nacional de Coordinación Antifraude; Fiscalía contra la Corrupción y la Criminalidad Organizada; Policía Nacional; Tribunal de Cuentas; y Defensor del Pueblo.
    - Canales europeos: Tribunal de Cuentas Europeo; y la Oficina Europea Antifraude.

5. Protección de datos personales

Régimen jurídico del tratamiento de datos

Los tratamientos de datos personales que deriven de la aplicación de la Ley 2/2023 se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, **RGPD**), en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, **LOPDGDD**), y en la **Ley Orgánica 7/2021**, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

No se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una información específica o, **si se recopilan por accidente, se eliminarán sin dilación indebida**.

Licitud de los tratamientos de datos

Se considerarán **lícitos los tratamientos de datos** personales necesarios para la **aplicación de esta Ley**, en virtud de lo que disponen los artículos **6.1.c) del RGPD**, **8 de la LOPDGDD**, y **11 de la Ley Orgánica 7/2021**, de 26 de mayo, dada la obligatoriedad por VIRTON, S.A., de disponer de un Sistema interno de información como entidad pública (de acuerdo a lo establecido en el art. 13 de esta Ley).

Información sobre protección de datos personales y ejercicio de derechos

Cuando se obtengan directamente de los interesados sus datos personales se les facilitará la información a que se refiere el art. 11 de la LOPDGDD y 13 del RGPD: **deber de información**.

Los interesados podrán **ejercer los derechos a que se refieren los artículos 15 a 22 del RGPD**:

- ✓ Derecho de acceso.
- ✓ Derecho de rectificación
- ✓ Derecho de supresión («el derecho al olvido»)
- ✓ Derecho de limitación del tratamiento
- ✓ Derecho a la portabilidad de los datos

- ✓ Derecho de oposición
- ✓ Derecho a decidir sobre tratamientos automatizados

Si **durante la tramitación** del procedimiento de estudio e investigación de las comunicaciones presentadas, la **persona afectada ejerciese el derecho de oposición, de rectificación o de supresión**, se presumirá que, salvo prueba en contrario, existen **motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales**.

Asimismo, el **derecho de acceso** para la persona afectada, **no comprenderá en ningún caso los relativos a la identidad del informante** y de otras personas afectadas por el procedimiento iniciado.

Por último, sin perjuicio de cualquier procedimiento administrativo o judicial, los interesados tienen derecho a quejarse ante las autoridades competentes, si piensan que el procesamiento de sus datos personales no se ha producido de conformidad con la LOPDGDD y el RGPD.

Tratamiento de datos personales en el Sistema interno de información.

El **acceso a los datos personales** contenidos en el Sistema interno de información quedará **limitado**, dentro del ámbito de sus competencias y funciones, exclusivamente a:

- ✓ El Responsable del Sistema y a quien lo gestione directamente.
- ✓ El Jefe de Sección de Recursos Humanos.
- ✓ La Dirección Gerencia.
- ✓ Los encargados del tratamiento que eventualmente se designen.
- ✓ El delegado de protección de datos.

Será **lícito el tratamiento** de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario **para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales** que, en su caso, procedan.

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.

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.

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

En todo caso, **transcurridos tres 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, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de la LOPDGDD.

Los datos personales relativos a las informaciones recibidas y a las investigaciones internas incluidas en el libro-registro sólo se conservarán durante el periodo que sea necesario y proporcionado a efectos de cumplir con las exigencias que establece la Ley 2/2023, estableciéndose, como periodo de conservación máximo a cualquier efecto, el plazo de diez años.

6. Control de versiones

Todos los cambios o actualizaciones serán reflejados en la siguiente tabla de control de versiones:

Versión	Autor	Descripción de las modificaciones	Aprobado por	Fecha*
V 1.0	Responsable del Sistema de información	Versión inicial del procedimiento	Consejo de Administración	07/04/2025

*Fecha del Consejo en el que se presenta el procedimiento para la aprobación de su nueva versión.

ANEXOS

Anexo 1: 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

Artículo 36

Prohibición de represalias

1. Se prohíben expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación conforme a lo previsto en esta ley.

2. Se entiende 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.

3. A los efectos de lo previsto en esta ley, y a título enunciativo, se consideran represalias las que se adopten en forma de:

a) Suspensión del contrato de trabajo, despido o extinción de la relación laboral o estatutaria, incluyendo la no renovación o la terminación anticipada de un contrato de trabajo temporal una vez superado el período de prueba, o terminación anticipada o anulación de contratos de bienes o servicios, imposición de cualquier medida disciplinaria, degradación o denegación de ascensos y cualquier otra modificación sustancial de las condiciones de trabajo y la no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido; salvo que estas medidas se llevaran a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral o reguladora del estatuto del empleado público correspondiente, por circunstancias, hechos o infracciones acreditadas, y ajenas a la presentación de la comunicación.

b) Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.

c) Evaluación o referencias negativas respecto al desempeño laboral o profesional.

d) Inclusión en listas negras o difusión de información en un determinado ámbito sectorial, que dificulten o impidan el acceso al empleo o la contratación de obras o servicios.

e) Denegación o anulación de una licencia o permiso.

f) Denegación de formación.

g) Discriminación, o trato desfavorable o injusto.

4. La persona que viera lesionados sus derechos por causa de su comunicación o revelación una vez transcurrido el plazo de dos años, podrá solicitar la protección de la autoridad competente que, excepcionalmente y de forma justificada, podrá extender el período de protección, previa audiencia de las personas u órganos que pudieran verse afectados. La denegación de la extensión del período de protección deberá estar motivada.

Anexo 2: Definiciones

- "**Ley 2/2023**"

  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**, que transpone la **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.

  La finalidad de la Ley 2/2023 es la de **proteger a las personas que en un contexto laboral o profesional detecten infracciones penales o administrativas graves o muy graves y las comuniquen mediante los mecanismos regulados en la misma**.

- "**Informante**"

  Es la persona que **comunica una infracción**.

- "**Afectado/Persona afectada**"

  Es la persona a la que se refieren los hechos relatados en la infracción comunicada por un informante.

- "**Infracción**"

  Actuación contraria al ordenamiento jurídico en general, al Código Ético de VIRTON S.A., y las políticas, procedimientos, instrucciones, etc. existentes en la Sociedad.

  La lista de infracciones a continuación no es exhaustiva, habrá muchas otras actuaciones que podrían plantearse y que no están recogidas:

  - Cuando se ha cometido/se está cometiendo/es probable que se cometa, una infracción penal o administrativa, grave o muy grave, de la normativa española o del Derecho de la Unión Europea;
  - Cuando una persona ha incumplido/está incumpliendo/es probable que incumpla, cualquier obligación legal distinta de las derivadas del contrato de trabajo;
  - Cuando se ha puesto/se está poniendo/es probable que se ponga en peligro, la salud y la seguridad de cualquier persona;
  - Cuando se ha dañado/se está dañando/pueda dañarse, el medio ambiente;
  - Cuando se ha producido/se está produciendo/es probable que se produzca, un uso ilegal o indebido de los fondos o recursos de un organismo público o de otros fondos públicos;
  - Cuando un acto u omisión por parte, o en nombre de un organismo público es opresivo, discriminatorio, gravemente negligente o constituye una mala administración grave;

- Cuando se ha incumplido/se está incumpliendo/es probable que se incumpla, el Código Ético de VIRTON S.A;
- Cuando se ha ocultado/se está ocultando/es probable que se oculte o destruya, cualquier asunto comprendido en alguno de los párrafos anteriores.

- "**Ámbito material de aplicación**" (art. 2 de la Ley)

  Proteger a las personas físicas que informen de:

  a) Cualesquiera acciones u omisiones que puedan constituir **infracciones del Derecho de la Unión Europea** siempre que:
  - **Entren dentro del ámbito de aplicación[6] de los actos de la Unión Europea enumerados en el anexo de la 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, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno;
  - **Afecten a los intereses financieros de la Unión Europea** tal y como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE); o
  - **Incidan en el mercado interior**, tal y como se contempla en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión Europea en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades o con prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades.

  b) Acciones u omisiones que puedan ser constitutivas de **infracción penal o administrativa grave o muy grave**. En todo caso, se entenderán comprendidas todas aquellas infracciones penales o administrativas graves o muy graves que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.

- **"Ámbito personal de aplicación"** (art. 3 de la Ley)

  Informantes que hayan obtenido información sobre infracciones en un **contexto laboral o profesional**:
  - Una persona física que es, o ha sido, empleada de VIRTON S.A, (trabajadores/as actuales o antiguos/as, a jornada completa o parcial);
  - Una persona física que trabaje, o haya trabajado, en virtud de cualquier contrato (escrito o verbal) como, por ejemplo, contratistas y consultores;

[6] Anexo 3: Directiva (UE) 2019/1937, art.2 "Ámbito de aplicación material"

- Una persona física que realice, o haya realizado, prácticas en el marco de un curso o programa de formación (becarios/as remunerados/as o no remunerados/as, estudiantes en prácticas, trabajadores/as eventuales, trabajadores/as de agencia);
- Una persona física que sea, o haya sido, voluntario/a;
- Una persona física que accede a información sobre una infracción relevante durante el proceso de contratación (solicitantes de empleo);
- Una persona física que accede a información sobre una infracción relevante durante las negociaciones precontractuales (distintas del proceso de contratación);
- Una persona física que sea, o haya sido, miembro de la Junta General;
- Una persona física que sea, o haya sido, miembro del Consejo de Administración;
- Personas físicas o jurídicas relacionadas con el informante.

- "**Sistema interno de información**" (art. 5 de la Ley)

  Todas las entidades que integran el **sector público** están **obligadas a disponer de un Sistema interno de información** en los términos previstos en la Ley 2/2023.

  El Sistema interno de información deberá cumplir con las condiciones previstas en el art. 5.2. de la Ley y se instrumenta en torno a cuatro elementos, que serán analizados a continuación en este procedimiento:

  - Estar diseñado, establecido y gestionado de una **forma segura**, de modo que se **garantice la confidencialidad** de la identidad del informante y de cualquier tercero mencionado en la comunicación, y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la **protección de datos**, impidiendo el acceso de personal no autorizado.
  - Contar con un **canal interno de información** que reúna todas las **garantías para la protección de los informantes**.
  - Contar con un **Responsable del Sistema interno de información.**
  - Contar con un **procedimiento de gestión de las informaciones** recibidas, diseñando y protocolizando las actuaciones a seguir.

- "**Canal interno de información**"

  Está i**ntegrado dentro del Sistema interno de información** y **posibilita la comunicación** de información respecto de:

  - Las (presuntas) infracciones previstas y descritas en el ámbito material de aplicación (Art. 7 de la Ley).
  - Cualesquiera otras infracciones o presuntos incumplimientos (actuaciones contrarias al ordenamiento jurídico, el Código Ético de VIRTON, S.A., sus políticas,

procedimientos, etc.), al tener conocimiento de los mismos o detectar indicios razonables de su comisión.

- "**Autoridad Independiente de Protección del Informante, A.A.I.**":
  - **Autoridad administrativa independiente**, con personalidad jurídica propia, plena capacidad de actuar de manera pública como privada, **con potestad administrativa, consultiva y sancionadora**.
  - Se configura como el **canal externo de información** al que pueden acudir los informantes para denunciar un delito que se esté produciendo dentro de VIRTON S.A., siempre que la infracción o delito denunciado afecte o produzca efectos **en el ámbito territorial de más de una comunidad autónoma.**
  - **Se regula en la Ley 2/2023**, en concreto en el Título VIII, artículos 42 a 59 y en un **futuro Estatuto**, para el que el Gobierno tiene el plazo de un año para elaborar.
  - Sus objetivos son **garantizar la confidencialidad y, en su caso, el anonimato de los informantes** de corrupción**, además de su protección frente a posibles represalias por denunciar conductas o acciones ilícitas dentro de sus organizaciones**.
- "**Partes interesadas**": cualquier parte, salvo los miembros de la organización, con quien la organización tiene, o prevé establecer, algún tipo de relación de negocios.

Anexo 3: 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

Artículo 2

Ámbito de aplicación material

1. **La presente Directiva establece normas mínimas comunes para la protección de las personas que informen sobre las siguientes infracciones del Derecho de la Unión**:

a) infracciones que entren dentro del ámbito de aplicación de los actos de la Unión enumerados en el anexo relativas a los ámbitos siguientes:

i) contratación pública,

ii) servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo,

iii) seguridad de los productos y conformidad,

iv) seguridad del transporte,

v) protección del medio ambiente,

vi) protección frente a las radiaciones y seguridad nuclear,

vii) seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales,

viii) salud pública,

ix) protección de los consumidores,

x) protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información;