Acuerdo del Consejo de Gobierno de la Universidad de Oviedo, de 26 de junio de 2023, por el que se aprueba la Política de protección de los informantes de infracciones normativas y corrupción

Contenido

1. Introducción 2
1.1. Finalidad de la Política 2
1.2. Ámbito personal de aplicación 2
2. **Sistema interno de información en la Universidad de Oviedo** 3
2.1. Comunicación de infracciones a través del Sistema interno de información. 3
2.2. Sistema interno de información 3
2.3. Gestión del Sistema interno de información por tercero externo 4
2.4. Canal interno de información 4
3. Publicidad del sistema y Registro de informaciones en la Universidad de Oviedo 7
3.1. Visibilidad de los canales interno y externo de información 7
3.2. Registro de informaciones 7
4. Protección de datos personales de los informantes en la Universidad de Oviedo 7
4.1. Régimen jurídico del tratamiento de datos personales 7
4.2. Tratamiento de datos personales en el Sistema interno de información 8
4.3. Preservación de la identidad del informante y de las personas afectadas 9
5. Medidas de protección de los informantes en la Universidad de Oviedo 9
5.1. Condiciones de protección 9
5.2. Prohibición de represalias 10
5.3. Medidas de apoyo 11
5.4. Medidas de protección frente a represalias 12
5.5. Supuestos de exención y atenuación de la sanción 12
6. Conclusiones: normas de organización del Sistema. 13

1. Introducción

1.1. Finalidad de la Política

El presente Acuerdo tiene por finalidad otorgar una protección adecuada por la Universidad de Oviedo y por sus medios propios frente a las represalias que puedan sufrir las personas físicas que informen sobre infracciones normativas o corrupción en el ámbito 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.

La protección del informante se articula sobre cuatro pilares: el canal interno de información, el responsable del sistema, el procedimiento de gestión de informaciones y el registro de informaciones. El incumplimiento de la obligación de disponer de un sistema interno de información en los términos exigidos está tipificado como infracción administrativa muy grave en el art. 63.1.g) de dicho texto legal, con una posible sanción de multa entre 600.001 y 1.000.000 de euros para las personas jurídicas [art. 65.1.b)].

1.2. Ámbito personal de aplicación

1. El presente Acuerdo se aplicará a los informantes que trabajen o hayan tenido una relación contractual de otro tipo en la Universidad de Oviedo o en sus medios propios, y que hayan obtenido información sobre infracciones en un contexto laboral o profesional.

2. El presente Acuerdo se aplicará a los informantes que comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral o estatutaria ya finalizada, voluntarios, becarios, trabajadores en periodos de formación con independencia de que perciban o no una remuneración, 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.

3. Las medidas de protección del informante también se aplicarán, en su caso, específicamente a los representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante.

4. Las medidas de protección del informante se aplicarán, en su caso, a:

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.

2. **Sistema interno de información en la Universidad de Oviedo**

2.1. Comunicación de infracciones a través del Sistema interno de información.

El Sistema interno de información es el cauce preferente para informar sobre las acciones u omisiones previstas, siempre que se pueda tratar de manera efectiva la infracción y si el denunciante considera que no hay riesgo de represalia.

2.2. Sistema interno de información

1. El Consejo de Gobierno será el responsable de la implantación del Sistema interno de información, 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.

En este sentido, la Ley establece en su artículo 5.1 que "el órgano de administración u órgano de gobierno de cada entidad será el responsable de la implantación del Sistema interno de información". Por su parte, la Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario (en adelante LOSU) define en su artículo 46.1 al Consejo de Gobierno como "máximo órgano de gobierno de la universidad", al que además corresponde "fijar las directrices fundamentales y los procedimientos de aplicación de todas las políticas de la universidad".

2. El Sistema interno de información de la Universidad, en cualquiera de sus fórmulas de gestión, deberá:

a) Permitir a todos los informantes comunicar las infracciones.

b) 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.

c) Permitir la presentación de comunicaciones por escrito o verbalmente, o de ambos modos.

d) Integrar los distintos canales internos de información que pudieran establecerse dentro de la entidad.

e) Garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la correspondiente entidad u organismo con el objetivo de que el primero en conocer la posible irregularidad sea la propia entidad u organismo.

f) Ser independientes y aparecer diferenciados respecto de los sistemas internos de información de otras entidades u organismos.

g) Contar con un responsable del sistema en los términos previstos en esta política.

h) Contar con una política o estrategia que enuncie los principios generales en materia de Sistemas interno de información y defensa del informante y que sea debidamente publicitada en el seno de la Universidad, ya a través del Diario de la Universidad de Oviedo, ya a través de un correo institucional.

i) Contar con un procedimiento de gestión de las informaciones recibidas.

j) Establecer las garantías para la protección de los informantes en el ámbito de la Universidad.

2.3. Gestión del Sistema interno de información por tercero externo

La gestión del Sistema interno de información se llevará a cabo por servicios de la Universidad, sin perjuicio de la posibilidad de externalizarla en los términos permitidos por la Ley. Dicha externalización requerirá consulta previa a la representación legal de las personas trabajadoras.

2.4. Canal interno de información

El canal interno deberá permitir realizar comunicaciones por escrito o verbalmente, o de las dos formas. La información se podrá realizar bien por escrito, a través de correo postal o a través de cualquier medio electrónico habilitado al efecto, o verbalmente, por vía telefónica o a través de sistema de mensajería de voz. A solicitud del informante, también podrá presentarse mediante una reunión presencial dentro del plazo máximo de siete días.

En su caso, se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo con la normativa vigente.

Además, a quienes realicen la comunicación a través de canales internos se les informará, de forma clara y accesible, sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

Al hacer la comunicación, el informante podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones.

Las comunicaciones verbales, incluidas las realizadas a través de reunión presencial, telefónicamente o mediante sistema de mensajería de voz, deberán documentarse de alguna de las maneras siguientes, previo consentimiento del informante:

a) mediante una grabación de la conversación en un formato seguro, duradero y accesible, o

b) 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.

Los canales internos de información permitirán incluso la presentación y posterior tramitación de comunicaciones anónimas.

2.5. Responsable del Sistema interno de información

Se designa «Responsable del Sistema» a la Comisión de Transparencia, Buen Gobierno y Protección de Datos. Salvo delegación de la Comisión en otro sentido, la persona física con facultades de gestión del Sistema y de tramitación de expedientes de investigación será el responsable de la unidad de transparencia, que actúa como Secretario de dicha Comisión.

Tanto el nombramiento como el cese de la persona física individualmente designada, deberán ser notificados a la Autoridad Independiente de Protección del Informante, A.A.I., o, en su caso, al órgano equivalente de la Comunidad Autónoma en el plazo de los diez días hábiles.

El Responsable del Sistema deberá desarrollar sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad u organismo, 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.

2.6. Procedimiento de gestión de informaciones

1.El Responsable del Sistema responderá de su tramitación diligente.

2. El procedimiento establecerá las previsiones necesarias para que el Sistema interno de información y los canales internos de información existentes cumplan con los requisitos establecidos en esta Ley. En particular, el procedimiento responderá al contenido mínimo y principios siguientes:

a) Identificación del canal o canales internos de información a los que se asocian.

b) Inclusión de información clara y accesible sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

c) 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.

d) Determinación del plazo máximo para dar respuesta a las actuaciones de investigación, que 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.

e) Previsión de la posibilidad de mantener la comunicación con el informante y, si se considera necesario, de solicitar a la persona informante información adicional.

f) 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.

g) Garantía de la confidencialidad cuando la comunicación sea remitida por canales de denuncia que no sean los establecidos o a miembros del personal no responsable de su tratamiento, al que se habrá formado en esta materia y advertido de la tipificación como infracción muy grave de su quebranto y, asimismo, el establecimiento de la obligación del receptor de la comunicación de remitirla inmediatamente al Responsable del Sistema.

h) Exigencia del respeto a la presunción de inocencia y al honor de las personas afectadas.

i) Respeto de las disposiciones sobre protección de datos personales.

j) Remisión de la información 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.

3. Publicidad del sistema y Registro de informaciones en la Universidad de Oviedo

3.1. Visibilidad de los canales interno y externo de información

La Universidad de Oviedo propiciará la información adecuada de forma clara y fácilmente accesible, sobre el uso de todo canal interno de información que hayan implantado, así como sobre los principios esenciales del procedimiento de gestión. Dicha información deberá constar en la página de inicio de la web institucional, en una sección separada y fácilmente identificable.

Como complemento, la Universidad, en su página específica de lucha contra la corrupción https://antifraude.uniovi.es, desarrollada en ejecución del Plan Antifraude para la gestión de los fondos europeos, también hará visible un enlace al canal de denuncias.

3.2. Registro de informaciones

1.La Universidad de Oviedo con un libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad previstos en esta ley.

Este registro no será público y únicamente a petición razonada de la autoridad judicial competente. En el marco de un procedimiento judicial y bajo la tutela de dicha autoridad, podrá accederse total o parcialmente al contenido del referido registro.

2. Los datos personales relativos a las informaciones recibidas y a las investigaciones internas a que se refiere el apartado anterior solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con la Ley. En ningún caso podrán conservarse los datos por un período superior a diez años.

4. Protección de datos personales de los informantes en la Universidad de Oviedo

4.1. Régimen jurídico del tratamiento de datos personales

Los tratamientos de datos personales que deriven de la aplicación de esta Política se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, 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, y en el presente título.

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.

4.2. Tratamiento de datos personales en el Sistema interno de información

1. 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:

a) El Responsable del Sistema y a quien lo gestione directamente.

b) El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador. En el caso de los empleados públicos, el órgano competente para la tramitación del mismo.

c) El responsable de los servicios jurídicos, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.

d) Los encargados del tratamiento que eventualmente se designen.

e) El delegado de protección de datos.

2. 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.

En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la ley.

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.

3. 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.

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.

4. 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 Ley Orgánica 3/2018, de 5 de diciembre.

5. Los empleados y terceros deberán ser informados acerca del tratamiento de datos personales en el marco del Sistema de información.

4.3. Preservación de la identidad del informante y de las personas afectadas

1. Quien presente una comunicación o lleve a cabo una revelación pública tiene derecho a que su identidad no sea revelada a terceras personas.

2. Los sistemas internos de información, los canales externos y quienes reciban revelaciones públicas no obtendrán datos que permitan la identificación del informante y deberán contar con medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado.

3. 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.

Las revelaciones hechas en virtud de este apartado estarán sujetas a salvaguardas establecidas en la normativa aplicable. En particular, se trasladará al informante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial. Cuando la autoridad competente lo comunique al informante, le remitirá un escrito explicando los motivos de la revelación de los datos confidenciales en cuestión.

5. Medidas de protección de los informantes en la Universidad de Oviedo

5.1. Condiciones de protección

1. Los informantes tendrán derecho a protección siempre que concurran las circunstancias siguientes:

a) 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,

b) la comunicación o revelación se haya realizado conforme a los requerimientos previstos en la Ley.

2. Quedan expresamente excluidos de la protección prevista en esta ley aquellas personas que comuniquen o revelen:

a) Informaciones contenidas en comunicaciones que hayan sido inadmitidas por algún canal interno de información.

b) Informaciones vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación o revelación.

c) Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores.

d) Informaciones que se refieran a acciones u omisiones no comprendidas en la Ley.

3. Las personas que hayan comunicado o revelado públicamente información sobre acciones u omisiones de forma anónima pero que posteriormente hayan sido identificadas y cumplan las condiciones previstas en la Ley, tendrán derecho a la protección que la misma contiene.

5.2. 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 la Ley.

2. En particular, 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.

5. Los actos administrativos que tengan por objeto impedir o dificultar la presentación de comunicaciones y revelaciones, así como los que constituyan represalia o causen discriminación tras la presentación de aquellas al amparo de esta ley, 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.

5.3. Medidas de apoyo

1. La Universidad prestará a los informantes las medidas de apoyo siguientes:

a) Información y asesoramiento completos e independientes, que sean fácilmente accesibles para el público y gratuitos, sobre los procedimientos y recursos disponibles, protección frente a represalias y derechos de la persona afectada.

b) Asistencia efectiva por parte de las autoridades competentes ante cualquier autoridad pertinente implicada en su protección frente a represalias, incluida la certificación de que pueden acogerse a protección al amparo de la presente ley.

c) Asistencia jurídica en los procesos penales y en los procesos civiles transfronterizos de conformidad con la normativa comunitaria.

d) Apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la Autoridad Independiente de Protección del Informante.

5.4. Medidas de protección frente a represalias

1. No se considerará que los informantes han infringido ninguna restricción de revelación de información, ni incurrirán en responsabilidad de ningún tipo en relación con dicha comunicación o revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública de dicha información era necesaria para revelar una acción u omisión. Esta medida no afectará a las responsabilidades de carácter penal.

Lo previsto en el párrafo anterior se extiende a la comunicación de informaciones realizadas por los representantes de las personas trabajadoras, aunque se encuentren sometidas a obligaciones legales de sigilo o de no revelar información reservada. Todo ello sin perjuicio de las normas específicas de protección aplicables conforme a la normativa laboral.

2. Los informantes no incurrirán en responsabilidad respecto de la adquisición o el acceso a la información que es comunicada o revelada públicamente, siempre que dicha adquisición o acceso no constituya un delito.

3. Cualquier otra posible responsabilidad de los informantes derivada de actos u omisiones que no estén relacionados con la comunicación o la revelación pública o que no sean necesarios para revelar una infracción en virtud de esta ley será exigible conforme a la normativa aplicable.

Durante la tramitación del expediente los informantes 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.

5.5. Supuestos de exención y atenuación de la sanción.

1. Cuando una persona que hubiera participado en la comisión de la infracción administrativa objeto de la información sea la que informe de su existencia mediante la presentación de la información y siempre que la misma hubiera sido presentada con anterioridad a que hubiera sido notificada la incoación del procedimiento de investigación o sancionador, el órgano competente para resolver el procedimiento, mediante resolución motivada, podrá eximirle del cumplimiento de la sanción administrativa que le correspondiera siempre que resulten acreditados en el expediente los siguientes extremos:

a) Haber cesado en la comisión de la infracción en el momento de presentación de la comunicación o revelación e identificado, en su caso, al resto de las personas que hayan participado o favorecido aquella.

b) Haber cooperado plena, continua y diligentemente a lo largo de todo el procedimiento de investigación.

c) Haber facilitado información veraz y relevante, medios de prueba o datos significativos para la acreditación de los hechos investigados, sin que haya procedido a la destrucción de estos o a su ocultación, ni haya revelado a terceros, directa o indirectamente su contenido.

d) Haber procedido a la reparación del daño causado que le sea imputable.

2. Cuando estos requisitos no se cumplan en su totalidad, incluida la reparación parcial del daño, quedará a criterio de la autoridad competente, previa valoración del grado de contribución a la resolución del expediente, la posibilidad de atenuar la sanción que habría correspondido a la infracción cometida, siempre que el informante o autor de la revelación no haya sido sancionado anteriormente por hechos de la misma naturaleza que dieron origen al inicio del procedimiento.

3. La atenuación de la sanción podrá extenderse al resto de los participantes en la comisión de la infracción, en función del grado de colaboración activa en el esclarecimiento de los hechos, identificación de otros participantes y reparación o minoración del daño causado, apreciado por el órgano encargado de la resolución.

6. Conclusiones: normas de organización del Sistema.

En función de todo lo expuesto, la presente Política se traduce en la necesidad de unas Normas de organización del Sistema Interno de Información, a saber:

Artículo 1. Objeto.

Las presentes Normas tienen por objeto regular el Sistema Interno de Información que se establece en la Universidad de Oviedo para dar efectividad a lo dispuesto por 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, Ley 2/2023).

Artículo 2. Sistema Interno de Información.

El Sistema Interno de Información de la Universidad de Oviedo, accesible desde el portal web institucional, es el cauce de comunicación adecuado para la recepción de información sobre hechos o conductas a los que se refiere la Ley 2/2023 y que guarden relación con la actividad y funcionamiento de la Universidad y sus medios propios.

Tendrán la condición de informantes los sujetos establecidos en el artículo 3 de la Ley 2/2023.

Artículo 3. Gestión del Sistema Interno de Información. Responsable.

1. El Sistema Interno de Información será gestionado por la Secretaría General de la Universidad de Oviedo y su Responsable será la Comisión de Transparencia, Buen Gobierno y Protección de Datos. Salvo delegación de la Comisión en otro sentido, la persona física con facultades de gestión del Sistema y de tramitación de expedientes de investigación será el responsable de la unidad de transparencia, que actúa como Secretario de dicha Comisión.

2. El Responsable desarrollará sus funciones con independencia funcional, no pudiendo recibir ningún tipo de instrucciones y disponiendo de los medios personales y materiales necesarios para poder llevar adecuadamente su función.

Artículo 4. Libro-registro de informaciones.

Se crea un libro-registro electrónico de las informaciones recibidas y de las labores de verificación a que hayan dado lugar, garantizándose, en todo caso, los requisitos de confidencialidad y de acceso restringido, todo ello en los términos del artículo 26 de la Ley 2/2023, de 20 de febrero.

Artículo 5. Garantía de confidencialidad.

1. El Responsable del Sistema deberá guardar el debido secreto respecto de cualquier información de la que tenga conocimiento como consecuencia de lo dispuesto en las presentes Normas. No podrá utilizar esta información para fines distintos de los expresamente establecidos por el ordenamiento jurídico.

2. Salvo cuando el informante solicite expresamente lo contrario, se guardará confidencialidad respecto de su identidad, de forma que la misma no será revelada a persona alguna. En todas las comunicaciones, actuaciones de verificación o solicitudes de documentación que se lleven a cabo se omitirán los datos relativos a la identidad del informante, así como cualesquiera otros que pudieran conducir total o parcialmente a su identificación.

3. Se guardará confidencialidad y se preservará la identidad de los afectados y de los terceros mencionados en la información remitida.

4. Sin perjuicio de lo establecido en los apartados anteriores, la identidad del informante, así como del afectado y de los terceros mencionados en la información remitida, podrá ser comunicada a la Autoridad Judicial, al Ministerio Fiscal y/o a la autoridad administrativa competente cuando, en el marco de una investigación penal, disciplinaria o sancionadora, así lo establezcan las Leyes.

Artículo 6. Procedimiento de gestión de las informaciones.

1. La remisión de la información acerca de la comisión de hechos o conductas a los que se refiere la Ley 2/2023 puede realizarse de forma anónima o con la identificación del informante. Se adoptarán las medidas organizativas y técnicas necesarias para preservar la identidad del informante.

2. La remisión de la información se realiza, por escrito, bien a través de la plataforma informática accesible desde el portal web de la Universidad, bien a través de correo postal o verbalmente, a través del número de teléfono o sistema de mensajería instantánea establecido a tal efecto. También, a solicitud del informante, podrá realizarse mediante reunión presencial con el Responsable del Sistema, que deberá tener lugar dentro de los cinco días hábiles siguientes a su solicitud.

3. Remitida la información o realizada la reunión presencial, se procederá a su registro en el Sistema de Gestión de Información. Se abrirá el oportuno expediente y se le asignará un código de identificación y seguimiento y procediendo a acusar recibo de la misma dentro de los cinco días hábiles siguientes, salvo que el informante haya renunciado expresamente a recibir cualesquiera comunicaciones del Responsable del Sistema.

Artículo 7. Admisión a trámite de la información.

1. El Responsable del Sistema comprobará si la información remitida relata hechos o conductas de los referidos en la Ley 2/2023, y decidirá sobre su admisión o inadmisión en un plazo no superior a diez días hábiles.

2. Serán causas de inadmisión las siguientes:

a) Que los hechos o conductas relatados carezcan manifiestamente de verosimilitud o fundamento.

b) Que los hechos o conductas relatados no entren dentro del ámbito de aplicación material de la Ley 2/2023 o que no guarden relación con la actividad y funcionamiento de la Universidad o sus medios propios.

c) Que los hechos o conductas relatados no contengan información nueva y significativa respecto de procedimientos terminados, salvo que se aprecien nuevas circunstancias de hecho o de derecho que justifiquen un nuevo procedimiento.

d) Que la información sobre los hechos o conductas relatados haya sido obtenida mediante la comisión de un delito. En este supuesto, además de la inadmisión, se remitirá la información recibida al Ministerio Fiscal.

e) Que los hechos o conductas relatados no guarden relación con la actividad y funcionamiento de la Universidad o sus medios propios. En este supuesto, se remitirá la información al órgano, autoridad o entidad que se considere competente para su tramitación.

3. La admisión o inadmisión se comunicará al informante dentro de los cinco días hábiles siguientes, salvo que el informante haya renunciado expresamente a recibir cualesquiera comunicaciones del Responsable del Sistema.

4. En aquellos supuestos en que los hechos relatados puedan ser indiciariamente constitutivos de ilícito penal, el Responsable del Sistema dará traslado inmediato de la información al Ministerio Fiscal.

Artículo 8. Labores de verificación.

1. Las labores de verificación del Responsable del Sistema comprenderán todas aquellas actuaciones encaminadas a comprobar los hechos o conductas relatados a los efectos de determinar el tratamiento que deban darse a los mismos. A tales efectos, podrá solicitar la documentación o información adicional que estime oportuno, tanto al informante como a las personas u órganos que pudieran disponer de la documentación o información adicional necesaria.

2. Se garantizará que el afectado por la información tenga noticia de la misma, así como de los hechos relatados de manera sucinta. Será informado, además, del derecho que tiene a presentar alegaciones por escrito y del tratamiento de sus datos personales.

3. Sin perjuicio del derecho a formular alegaciones por escrito, las labores de verificación comprenderán, siempre que sea posible, una entrevista con el afectado en la que, con absoluto respeto a la presunción de inocencia, se le invitará a exponer su versión de hechos y a aportar los medios de prueba que considere adecuados y pertinentes.

El afectado tendrá acceso al expediente. Se omitirán, en su caso, los elementos que coadyuven a la identificación del informante. El afectado podrá, además, ser oído en cualquier momento y será advertido de la posibilidad de comparecer asistido de abogado.

Artículo 9. Terminación de las actuaciones.

1. Concluidas las labores de verificación, el Responsable del Sistema emitirá un informe en el que, además de la exposición de los hechos o conductas relatados, el número de expediente, el código de identificación de la información y la fecha de registro, las labores de verificación practicadas y las conclusiones alcanzadas mediante la valoración de las diligencias practicadas y de los indicios que las sustentan, adoptará alguna de las siguientes decisiones:

a) Archivo del expediente, cuando del procedimiento seguido no quepa advertir la comisión de hechos o conductas de los referidos por la Ley 2/2023 y que guarden relación con la actividad y funcionamiento universitario.

b) Remisión de la información, así como del informe final, al órgano competente para perseguir los hechos o conductas a los que se refiere la Ley 2/2023. Cuando pudiera proceder la adopción de medidas disciplinarias contra un empleado público de la Universidad, el informe se remitirá a la Secretaría General. Cuando se aprecie que los hechos o conductas pudieran ser indiciariamente constitutivos de ilícito penal, el informe se remitirá al Ministerio Fiscal. En el resto de los casos, el informe se remitirá a la Autoridad Independiente de Protección del Informante.

2. El plazo para finalizar el procedimiento y dar, en su caso, respuesta al informante no podrá ser superior a los tres meses desde la recepción de la información. La decisión adoptada en el informe final será notificada, en su caso, al informante y al afectado.

Artículo 10. Informe anual del Responsable del Sistema.

El Responsable del Sistema elaborará un informe anual de seguimiento de las presentes Normas para la Comisión de Transparencia, Buen Gobierno y Protección de Datos, pudiendo incluir propuestas de mejora y actualización. Dicho informe se pondrá a disposición de la representación legal de las personas trabajadoras.