AUDITORIA • CONSULTORIA

SISTEMA INTERNO DE INFORMACIÓN
(Manual de uso)

Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre las infracciones normativas y de lucha contra la corrupción.

A member of Nexia International

Índice de revisiones

HISTORIAL DE VERSIONES DEL MANUAL DE USO DEL SISTEMA INTERNO DE INFORMACIÓN				
Versión del manual	Fecha aprobación y actualización	Entrada en vigor	Órgano de aprobación	Epígrafes modificados
V.2023.1	20/11/2023	01/12/2023	Órgano de administración	Primera versión
-	-	-	-	-
-	-	-	-	-

Índice

0. Introducción y origen ... 3
1. Identificación de la entidad ... 5
2. Obligatoriedad de disponer del Sistema Interno de Información ... 5
3. Finalidad y principios esenciales del Sistema Interno de Información de AUDRIA ... 6
4. Contexto ... 7
4.1. Necesidades y expectativas de las partes interesadas ... 8
4.2. Determinación del alcance del Sistema Interno de Información ... 9
Ámbito material ... 9
Ámbito personal ... 10
Canal de comunicación ... 11
5. Liderazgo y compromiso ... 12
5.1. Responsable del Sistema Interno de Información ... 12
6. Política del Sistema Interno de Información ... 14
7. Sistema de gestión de comunicaciones ... 15
7.1. Vías de comunicación y/o información ... 15
7.2. El informante ... 16
7.3. Protección de Datos Personales ... 19
8. Planificación ... 20
8.1. Acciones para abordar riesgos y oportunidades ... 20
8.2. Objetivos del sistema de gestión de comunicaciones y planificación para alcanzarlos 21
9. Apoyo ... 22
9.1. Recursos ... 22
9.2. Competencia del Responsable del Sistema ... 22
9.3. Toma de conciencia y formación ... 23
9.4. Comunicación ... 23
10. Evaluación y revisión ... 24
10.1 Evaluación del desempeño ... 24
10.2. Mantenimiento de registros ... 24
10.3. Auditoría interna ... 25
11. Aprobación del Sistema Interno de Información ... 26

ANEXOS 27
ANEXO I - Matriz partes interesadas 28
ANEXO II – Formulario de comunicación del Responsable del SII a la AAI 29
ANEXO III – Política del Sistema Interno de Información 43
ANEXO IV - Protocolo del canal de comunicación 46
Anexo IV.1 - DECLARACIÓN DE AUSENCIA DE CONFLICTOS DE INTERESES (DACI) 58
Anexo IV.2 - ACUERDO DE CONFIDENCIALIDAD 60
Anexo IV.3 - MANUAL DE USO DE LA HERRAMIENTA DE CANAL DE INFORMACIÓN "OVET AUKI" 65

0. Introducción y origen

De la directiva (UE) *Whistleblowing* a la ley 2/2023

En octubre del 2019, la Unión Europea aprobó la Directiva (UE) 2019/1937 relativa a la protección de las personas que informen sobre infracciones del derecho de la Unión, comúnmente conocida como "Directiva *Whistleblowing*", normativa que nació con el fin de proteger a las personas que informen sobre irregularidades, infracciones o delitos dentro de las empresas pertenecientes a la Unión Europea.

A este respecto, el objeto de dicha Directiva se determinó en su artículo 1, disponiendo lo siguiente: *"La presente Directiva tiene por objeto reforzar la aplicación del Derecho y las políticas de la Unión en ámbitos específicos mediante el establecimiento de normas mínimas comunes que proporcionen un elevado nivel de protección de las personas que informen sobre infracciones del Derecho de la Unión."*

Ley de Protección al Informante en España

Con la entrada en vigor de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción – en lo sucesivo, 'Ley de Protección al Informante' o 'Ley 2/2023' – se transpuso en el ordenamiento jurídico español la Directiva Whistleblowing, anteriormente mencionada.

La finalidad de la norma, determinada en su título I, 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. Con esta finalidad de protección, se espera que se apliquen las disposiciones de la norma para el diseño, implantación y gestión de los sistemas de información.

Asimismo, la Ley de Protección al informante también tiene como propósito el fortalecimiento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público.

Por todo ello, la norma obliga – a determinados sujetos – a contar con un Sistema Interno de Información, así como un sistema de gestión y protección de los informantes, evitando represalias sobre ellos.

Las principales novedades que introduce la Ley 2/2023 son las siguientes:

- Amplía el ámbito de aplicación de la Directiva *Whistleblowing* respecto del tipo de comunicaciones que generan el derecho de protección.
- Obliga a implementar canales internos de información a las entidades públicas y a determinadas entidades privadas que deberán cumplir unos requisitos y garantías mínimas.
- Requiere la tramitación efectiva de las comunicaciones, en la que también habrá que respetar una serie de garantías y derechos mínimos.

- Se exige la integración de todos los canales de las entidades en un único Sistema Interno de Información, garantizando así que la recepción y tramitación de todas las comunicaciones sobre potenciales infracciones cumplan las exigencias de la Ley 2/2023.
- Se exige que las entidades admitan y tramiten comunicaciones anónimas.
- Determina la creación de la Autoridad Independiente de Protección al Informante (en adelante A.I.I.), con potestades sancionadoras en esta materia y con responsabilidades de gestión del canal externo de comunicaciones que también crea la ley, así como de las medidas de apoyo a los informantes, entre otras funciones.
- Legitima la revelación pública de las infracciones en determinados supuestos.
- Impone la obligación al órgano de administración o de gobierno de designar a un responsable del sistema de información interno.
- Las medidas de protección no se limitan exclusivamente a la prohibición de represalias, sino también a medidas de tipo asistencial.

¿Qué obligaciones origina la entrada en vigor de la Ley 2/2023?

A lo largo del presente documento, se irán definiendo y desarrollando las diferentes obligaciones que con la entrada en vigor de la Ley de Protección del Informante se originaron, siendo principalmente las que se enumeran a continuación:

- Crear un Sistema Interno de Información (canal interno) seguro, que tiene que contar con las medidas técnicas y organizativas adecuadas para preservar la identidad del informante y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero.
  También tiene que garantizar la presentación y tramitación de comunicaciones anónimas.

- Informar de forma fácil y accesible sobre la existencia, el uso y el funcionamiento del canal interno de información, para que aquellas personas que estén considerando la posibilidad de realizar una comunicación, puedan tomar una decisión fundamentada sobre su conveniencia, y; cómo y cuando realizarla.

- Regular el procedimiento de gestión del canal para la tramitación diligente de las informaciones o comunicaciones de conformidad con la Ley y definir una política o estrategia que tiene que ser dada a conocer dentro de la organización.

- Designar un responsable del Sistema Interno de Información, que puede ser una persona física o un órgano colegiado.

- Comunicar a la Autoridad competente la designación del responsable del Sistema Interno de Información.

- Contar con un libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar.

- Informar, de forma clara y accesible, a quién realice la comunicación a través del canal interno sobre la existencia del canal externo.

1. Identificación de la entidad

El presente Sistema Interno de Información – en adelante "SII" o "el Sistema" – ha sido confeccionado por la entidad que se identifica a continuación, cuya finalidad es la de dar cumplimiento a la Ley 2/2023.

DENOMINACIÓN SOCIAL	**AUDRIA AUDITORÍA Y CONSULTORÍA, S.L.P.**
NIF	B65732141
OBJETO SOCIAL	La prestación de servicios profesionales propios de la actividad de miembro colegiado del Registro Oficial de Auditores de Cuentas del Instituto de Contabilidad y Auditoría de Cuentas y el ejercicio profesional derivado de la actividad de miembro colegiado del Colegio de Economistas de España y del Instituto de Censores Jurados de Cuentas de España.
UBICACIÓN	Gran Vía de les Corts Catalanes, 645, 6º 2ª – 08010 - Barcelona

2. Obligatoriedad de disponer del Sistema Interno de Información

El capítulo II de la Ley de protección al informante delimita las entidades que están obligadas a disponer de un Sistema Interno de Información en los términos previstos en la citada norma.

AUDRIA AUDITORÍA Y CONSULTORÍA, S.L.P., en adelante AUDRIA, por su consideración de sujeto obligado de las disposiciones aplicables en materia de prevención del blanqueo de capitales y de la financiación del terrorismo y de conformidad con lo dispuesto por el artículo 10.1 b) de la Ley 2/2023, tiene la obligación de disponer del citado Sistema Interno de Información, que será desarrollado en los distintos apartados del presente documento.

Artículo 10. Entidades obligadas del sector privado.

"1. Estarán obligadas a disponer un Sistema Interno de Información en los términos previstos en esta ley:

(...) b) Las personas jurídicas del sector privado que entren en el ámbito de aplicación de los actos de la Unión Europea en materia de servicios, productos y mercados financieros, prevención del blanqueo de capitales o de la financiación del terrorismo, seguridad del transporte y protección del medio ambiente a que se refieren las partes I.B y II del anexo de la Directiva (UE) 2019/1937, del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, deberán disponer de un Sistema Interno de Información que se regulará por su normativa específica con independencia del número de trabajadores con que cuenten. En estos casos, esta ley será de aplicación en lo no regulado por su normativa específica.

Se considerarán incluidas en el párrafo anterior las personas jurídicas que, pese a no tener su domicilio en territorio nacional, desarrollen en España actividades a través de sucursales o agentes o mediante prestación de servicios sin establecimiento permanente."

3. Finalidad y principios esenciales del Sistema Interno de Información de AUDRIA

Como se ha detallado anteriormente, la finalidad principal de la Ley 2/2023 es otorgar una protección adecuada frente a las represalias que pueden llegar a sufrir las personas físicas cuando informen de una acción u omisión especificada en el apartado 4.2. del presente documento.

Asimismo, también persigue fortalecer la cultura de la información de la infraestructura de integridad de las organizaciones y el fomento de la información o comunicación como mecanismo para prevenir y detectar amenazas con un interés de carácter público.

En la misma línea, los principios esenciales del Sistema Interno de Información pueden sintetizarse en:

- El fomento y fortalecimiento de la cultura de la información.
- El fomento de la integridad y ética empresarial.
- La prevención de la corrupción.
- El compromiso con la transparencia y la integridad.
- El fomento de la confianza en el mercado.
- La garantía de confidencialidad de la identidad del informante y de cualquier tercero mencionado, así como del tratamiento de la información y su investigación.
- Asegurar la protección adecuada frente a la adopción de represalias.
- El respeto al principio de presunción de inocencia y derecho de defensa de las partes afectadas.
- La garantía de independencia, imparcialidad y ausencia de conflictos de interés.
- La tramitación efectiva de las comunicaciones.
- La integración de la totalidad de los canales internos operativos en la entidad para la comunicación de posibles infracciones en un único canal de comunicación.

La implementación del Sistema Interno de Información está compuesta por:

1. El canal interno de recepción de informaciones o comunicaciones.
2. Las políticas que enuncian los principios generales en materia del Sistema Interno de Información y de defensa del informante y el procedimiento de gestión que establece las garantías para la protección de los informantes en el ámbito de la entidad.
3. Una persona responsable de la gestión y tramitación (Responsable del Sistema Interno de Información).

Como se ha señalado, el Sistema ofrece plenas garantías de independencia, confidencialidad, seguridad y garantiza evitar represalias a los informantes.

IMPORTANTE:

El Sistema Interno de Información constituirá el **cauce preferente** para la comunicación y tramitación de información (frente al canal externo o la revelación pública).

4. Contexto

AUDRIA es una firma de auditores y asesores de empresa con más de 30 años de experiencia que trabaja para que las empresas sean competitivas, afronten el futuro bien posicionadas y en el día a día distingan lo urgente de lo importante.

Para la firma, ofrecer un servicio profesional significa solucionar problemas, detectar oportunidades y convertir el consejo en acción.

Abogan por una atención adaptada a la necesidad de cada cliente, al que aportan valor mediante los principios de conocimiento y experiencia. La dimensión de la firma y un uso intensivo de las nuevas tecnologías les ayuda a mantener la cercanía con los clientes y a disponer de información actualizada en todo momento.

AUDRIA cuenta con un equipo multidisciplinar, que combina formación, trayectoria profesional, adaptabilidad, respuesta hacia retos imprevistos, capacidad técnica e implicación con el entorno social y económico.

AUDRIA tiene un programa de formación interna e incorpora los mejores profesionales para poder ofrecer en todo momento el servicio que el mercado demanda y la legislación, siempre cambiante, obliga. Formar parte de NEXIA y los programas de homogenización de servicios y de investigación de elevados estándares de calidad les permite garantizar una atención global de la máxima calidad.

La estructura participativa actual de AUDRIA es la siguiente:

En la elaboración del presente manual se han tenido en consideración entre otros, los siguientes factores:

a) el tamaño y la estructura de la organización;
b) las ubicaciones y sectores en los que la organización opera o prevé operar;
c) la naturaleza y alcance de relaciones comerciales con terceras partes;
d) cultura de cumplimiento;
e) estructuras, políticas, procesos, procedimientos y recursos internos (+ tecnológicos).

4.1. Necesidades y expectativas de las partes interesadas

En lo relativo a esta cuestión, la entidad ha confeccionado una matriz de partes interesadas, en la cual se definen los siguientes ítems (mínimos):

a) Identificación de las partes interesadas para el Sistema Interno de Información;
b) Identificación de las necesidades y las expectativas de las partes interesadas;
c) Identificación de las principales obligaciones del Sistema Interno de Información.

Respecto esta última cuestión, AUDRIA ha determinado, en el marco con las que la entidad mantiene relaciones contractuales, laborales o de otro tipo, a las siguientes partes interesadas:

- Clientes
- Trabajadores/personal
- Socios
- Administraciones Públicas

Se adjunta como **ANEXO I** la matriz de partes interesadas.

4.2. Determinación del alcance del Sistema Interno de Información

En el proceso de determinación del alcance del Sistema Interno de Información, AUDRIA ha tenido en consideración los apartados siguientes:

Ámbito material

El presente Sistema Interno de Información, abarca los siguientes ámbitos materiales de aplicación:

- **Hechos o conductas que puedan tener trascendencia penal.**
- **Infracciones administrativas graves o muy graves.**
- **Infracciones del Derecho laboral en materia de seguridad y salud en el trabajo** (sin perjuicio de la establecida en su normativa específica)**.**
- **Infracciones del Derecho de la Unión Europea incluidas en el ámbito material de aplicación 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 y la Ley española de transposición:**
  - ✓ **Contratación pública.**
  - ✓ **Servicios, productos y mercados financieros.**
  - ✓ **Seguridad de los productos y conformidad.**
  - ✓ **Seguridad del transporte.**
  - ✓ **Protección del medio ambiente.**
  - ✓ **Protección frente a las radiaciones y seguridad nuclear.**
  - ✓ **Seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales.**
  - ✓ **Salud pública.**
  - ✓ **Protección de los consumidores.**
  - ✓ **Protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información.**
  - ✓ **Prevención del blanqueo de capitales y la financiación del terrorismo → Información relevante sobre posibles incumplimientos, cometidos en el seno de la entidad, de:**
    - o La Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
    - o Su normativa de desarrollo (Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo).
    - o Las políticas y procedimientos implantados para darles cumplimiento (Manual de prevención del blanqueo de capitales y de la financiación del terrorismo).

- **Infracciones relativas al mercado interior, con inclusión de:**
  - ✓ **Infracciones de las normas de la Unión en materia de competencia y ayudas otorgadas por los estados.**
  - ✓ **Infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades (IS).**
  - ✓ **Prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable del impuesto sobre sociedades (IS).**
- **Infracciones – fraude y toda actividad ilegal – que afecte a los intereses financieros de la Unión Europea**
- **Cualquier otro tipo de irregularidad grave o muy grave que pueda implicar responsabilidad para AUDRIA.**
- **Prevención del acoso sexual y por razón de sexo, según lo estipulado en la normativa vigente de aplicación (Ley Orgánica 3/2007, para la igualdad efectiva de mujeres y hombres, artículo 48) y en el Protocolo de Prevención del Acoso Sexual y por Razón de Sexo de AUDRIA.**

IMPORTANTE

Cualesquiera otras comunicaciones, informaciones, quejas o sugerencias fuera del ámbito establecido en el presente subapartado serán desestimadas y tanto las mismas como sus remitentes quedarán fuera del ámbito de protección dispensado por el Sistema Interno de Información.

Ámbito personal

Pueden hacer uso del canal interno de comunicación y beneficiarse de la protección que otorga la Ley 2/2023 como informante, aquellas personas que tienen una **relación laboral o profesional** con AUDRIA, para comunicar información sobre las acciones u omisiones descritas en el artículo 2 de la Ley 2/2023 (enumeradas anteriormente en el ámbito de aplicación material).

En todo caso y a efectos de la citada Ley 2/2023, AUDRIA ha delimitado como eventuales comunicantes a:

- Las personas que tengan la condición de trabajadores por cuenta ajena, voluntarios, becarios y personas en formación – con independencia de que perciban o no una remuneración – e independientemente de su posición funcional y jerárquica, y de si la relación está vigente o finalizada.
  Aquellas personas que participen en el marco de procesos de selección (pero únicamente respecto aquellos casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual).
- Los autónomos.

- Los accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de la empresa.
- Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.
- Las personas físicas o jurídicas que, sin estar incluidas en los supuestos anteriores, hayan obtenido información sobre infracciones en el contexto de una relación profesional, administrativa, mercantil o de otro tipo con AUDRIA.

A este respecto, las medidas de protección al informante también se aplicarán, en su caso a:

- Los representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante.
- Las personas físicas que, en el marco de la organización en la que preste servicios al informante, asistan al mismo en el proceso.
- Las personas físicas que estén relacionadas con el informante y que puedan sufrir represalias como, por ejemplo, compañeros de trabajo o familiares.
- 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[1].

Los informantes pueden comunicar o informar acerca de acciones u omisiones indicadas en el ámbito de aplicación material del presente manual a través del canal que integra el Sistema Interno de Información.

Canal de comunicación

En el apartado 7.1 del presente documento se precisan las vías de comunicación habilitadas.

[1] 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.

5. Liderazgo y compromiso

Para que el sistema sea eficaz y tenga credibilidad, hace falta que toda comunicación pueda ser tratada de forma efectiva dentro de la propia organización. Por ello, resulta indispensable para la eficacia del Sistema Interno de Información, la designación adecuada del responsable.

A este respecto, el órgano de administración de la entidad será el responsable de la implantación del Sistema Interno de Información, previa consulta con la representación legal de las personas trabajadoras.

Nombramiento y cese del responsable del Sistema Interno de información

El órgano de administración de AUDRIA será el competente para la designación de la persona física responsable de la gestión de dicho sistema (Responsable del Sistema), siempre previa aceptación del cargo por la persona designada en cuestión, y habiendo comprobado que cumple con los requisitos que exige tanto la Ley 2/2023 como la política interna de AUDRIA.

Asimismo, el órgano de administración también tiene atribuida la potestad de su destitución y cese, por causas justificadas o a petición del Responsable del SII inicialmente designado.

5.1. Responsable del Sistema Interno de Información

En las entidades del sector privado, el responsable del Sistema debe ser un/a directivo/a, que ejercerá el cargo con **independencia** del órgano de administración.

Aun así, en caso de que por dimensiones o estructura de la entidad no sea posible, la Ley permite el desempeño ordinario de las funciones del cargo con las de responsable del Sistema, tratando en todo caso de evitar posibles **situaciones de conflicto de interés**.

Según lo expuesto anteriormente y por la naturaleza de la entidad, AUDRIA ha tomado la decisión de designar a como Responsable del Sistema Interno de Información a:

Nombre	Cargo en la organización
JUAN LUIS CASANOVA	Presidente

El Responsable del Sistema fue designado por el órgano de administración en el Acta de fecha 20 de noviembre de 2023.

Las personas incluidas en el ámbito de aplicación de la presente Política están obligadas a colaborar con la Responsable del Sistema, en los términos del presente manual.

Comunicación a la Autoridad Independiente de Protección al Informante

La designación del Responsable del Sistema debe ser notificada a la Autoridad Independiente de Protección al Informante (en adelante, A.A.I.) o, a las autoridades u órganos competentes de las comunidades autónomas.

En este sentido, la Oficina Antifraude de Cataluña, con su experiencia y conocimiento en la lucha contra la corrupción, ha asumido la responsabilidad de la AAI, convirtiéndose en la institución encargada de garantizar la protección y promoción de los derechos de los informantes en Cataluña.

De acuerdo con el artículo 8.3 de la Ley 2/2023, tanto el nombramiento como el cese de la persona física individualmente designada como Responsable del Sistema, así como, en su caso, los integrantes del órgano colegiado, deberán ser notificados a la Oficina Antifraude de Cataluña en el plazo de los 10 días hábiles siguientes del nombramiento o del cese, especificando, en el caso del cese, las razones que lo justifican.

Por lo anterior, la Oficina Antifraude dispone de un formulario con el fin de facilitar dichas comunicaciones, el cual se adjunta como **ANEXO II** del presente documento. Este formulario, se deberá presentar a través del Registro general de la sede electrónica de la Oficina Antifraude de Cataluña, a la cual se puede acceder mediante el siguiente enlace: https://seuelectronica.antifrau.cat/ca/registre-general.html

Otras cuestiones que tener en consideración

La persona responsable del Sistema Interno de Información también es responsable de la tramitación diligente de la alerta. Por eso es indispensable que pueda desarrollar sus funciones de forma independiente y autónoma, sin estar sujeta a ningún tipo de instrucción y contando con todos los medios personales y materiales necesarios para llevarlas a cabo.

6. Política del Sistema Interno de Información

AUDRIA cuenta con una Política del Sistema Interno de Información entendida como el documento en el cual se plasman los principios generales en materia de Sistema Interno de Información y defensa del informante y que debe ser debidamente publicitada en el seno de la organización.

Cabe poner de manifiesto que la citada Política es el pilar esencial del Sistema Interno de Información, precisando su aprobación por el Órgano de Gobierno y debiendo ser puesta a disposición de todas las personas a las que afecten. Por este motivo, AUDRIA ha determinado las siguientes vías de difusión:

- Publicación en la página web corporativa.
- Circular interna al personal de la organización.
- Email informativo a los socios de AUDRIA.

Se adjunta la Política del Sistema interno, aprobada por el Órgano de Gobierno, como **ANEXO III**

Asimismo, esta política debe:

- Estar alineada con los valores, objetivos u estrategia de la organización.
- Requerir el cumplimiento de las obligaciones de la organización.
- Apoyar los principios de la organización.
- Hacer referencia al Responsable del Sistema interno.
- Resumir las consecuencias de no cumplir con las obligaciones, las políticas, los procesos y los procedimientos de la organización.
- Fomentar el planteamiento de inquietudes y prohibir cualquier tipo de represalia.
- Estar escrita en un lenguaje sencillo de forma que todas las personas puedan entender fácilmente los principios y su intención.
- Implementarse y hacerse cumplir de forma adecuada.
- Estar disponible como información documentada.
- Estar disponible para las partes interesades, según corresponda.

7. Sistema de gestión de comunicaciones

La Ley 2/2023 determina los requisitos mínimos que debe cumplir la organización en relación con el Sistema Interno de Información. En concreto, en su artículo 7 y 9 se especifican las diferentes obligaciones.

La información puede comunicarse a AUDRIA de forma anónima. En otro caso, se reservará la identidad del informante de forma confidencial y quedará limitada al conocimiento del Responsable del Sistema Interno de Información.

La información se comunicará a través del canal interno de información, mediante la plataforma electrónica específica para tal fin, denominada "OVET AUKI" y a la que se puede acceder a través del siguiente enlace:

https://www.ovetauki.com/index.php?route=login/complaint&c_key=cexJzyREKMqqzuuBRjhAWVDWFQcjyAtoYnCp

Dicha plataforma electrónica permite la realización de comunicaciones escritas o verbales (en este último caso, adjuntando la grabación de la comunicación verbal).

Por otra parte, 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 formas siguientes, previo consentimiento del informante:

- Mediante una grabación de la conversación en un formato seguro, duradero y accesible,
- A través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.

Las informaciones recibidas por cualquier otro medio en AUDRIA, relacionadas con el objeto de la Ley 2/2023 se remitirán al canal interno de información bajo la administración del Responsable del Sistema Interno de Información.

En cualquier caso, los canales de comunicación estarán integrados dentro del Sistema Interno de información.

7.1. Vías de comunicación y/o información

Teniendo en consideración lo detallado con anterioridad, AUDRIA permite realizar comunicaciones de las siguientes formas;

a) Por escrito

- Correo postal (domicilio social de la entidad).
- Plataforma electrónica (Ovet Auki) alojada en la web www.audria.es

b) Verbalmente.

- Presencialmente: a solicitud del informante, podrá presentarse mediante una reunión presencial que tendrá lugar en un plazo máximo de 7 días. En este caso, se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo a lo que establece el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Asimismo, se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.
- Telefónicamente.
- Mensajería de voz.

El Protocolo del canal de comunicación, incorporado como **ANEXO IV** del presente documento, desarrolla el método de realización de comunicaciones por las distintas vías.

7.2. El informante

¿Cuándo se protegerá al informante?

Se protegerá al informante siempre que la comunicación o información se englobe dentro del ámbito de aplicación objetivo (o material) delimitado en el apartado 4.2 del presente documento.

Asimismo, en relación con las revelaciones públicas de la información, el artículo 28 de la Ley 2/2023 especifica que el informante estará protegido en los supuestos siguientes:

- Cuando la persona haya presentado una comunicación por canales internos y externos o directamente por canales externos y no se hayan tomado medidas adecuadas en los plazos establecidos.
- Cuando la persona tenga motivos razonables para pensar que la infracción puede constituir un peligro inminente o manifiesto para el interés público (en particular cuando se da una situación de emergencia), o existe un riesgo de daños irreversibles, incluido un peligro para la integridad física de una persona.
- Cuando la persona tenga motivos razonables para pensar que, si presenta una comunicación externa, hay riesgo de represalias o hay pocas probabilidades que se dé un tratamiento efectivo de la información, de conformidad con las circunstancias particulares del caso.

De igual forma, es conveniente poner de manifiesto que las condiciones para acogerse a la protección prevista no serán exigibles cuando la persona haya revelado información directamente a la prensa con arreglo al ejercicio de la libertad de expresión y de información veraz previstas constitucionalmente y en su legislación de desarrollo.

¿Qué excluye la Ley de su ámbito de protección?

A continuación, se enumeran las diferentes comunicaciones en las que no se ofrecerá protección ni al informante ni a las informaciones obtenidas al efecto:

- Los hechos comunicados carecen de toda verosimilitud o fundamento.
- Los hechos no son constitutivos de infracción al ordenamiento jurídico, de conformidad con en el ámbito de aplicación de la Ley 2/2023.
- Rumores.
- Conflictos interpersonales.
- Hechos que solo afectan al informante.
- Informaciones que no aporten nada nuevo o significativo a la inicial.
- Información obtenida mediante la comisión de un delito. En este supuesto, además, deberán remitirse con carácter inmediato los hechos constitutivos de delito a la Fiscalía.

Represalias y medidas de soporte

Como se ha puesto de manifiesto a lo largo del presente documento, una de las finalidades que persigue la Ley 2/2023 es la protección adecuada frente a posibles represalias, para fortalecer así la cultura de la información, de las infraestructuras de integridad de las organizaciones y el fomento de la cultura de la información como mecanismo para prevenir y detectar amenazas al interés público.

Por ello, la Ley 2/2023 incorpora un artículo específico – art. 36 – de prohibición de represalias, que determina lo siguiente:

- 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.

<u>¿Qué tiene la consideración de represalia?</u>

- 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.
- Se consideran represalias las que se adopten en forma de:
    - 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.

- Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.
- Evaluación o referencias negativas respecto al desempeño laboral o profesional.
- 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.
- Denegación o anulación de una licencia o permiso.
- Denegación de formación.
- Discriminación, o trato desfavorable o injusto.

Acciones que realizar y medidas de soporte

- 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.
- 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.
- La Autoridad Independiente de Protección del Informante podrá, en el marco de los procedimientos sancionadores que instruya, adoptar medidas provisionales en los términos establecidos en el artículo 56 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

A este respecto, la Ley 2/2023, en su artículo 37 delimita las medidas de apoyo para las personas que comuniquen o revelen infracciones – dentro del ámbito de aplicación material – a través del procedimiento previsto, siendo las siguientes:

- 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.
- 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.
- Asistencia jurídica en los procesos penales y en los procesos civiles transfronterizos de conformidad con la normativa comunitaria.
- Apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la A.A.I. tras la valoración de las circunstancias derivadas de la presentación de la comunicación.

Todo ello, con independencia de la asistencia que pudiera corresponder al amparo de la Ley 1/1996, de 10 de enero, de asistencia jurídica gratuita, para la representación y defensa en procedimientos judiciales derivados de la presentación de la comunicación o revelación pública."

7.3. Protección de Datos Personales

Los tratamientos de datos personales que deriven de la aplicación de la Ley 2/2023 se regirán por lo dispuesto en el RGPD y en la Ley Orgánica 3/2018, de 5 diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDPGDD).

El Sistema Interno de Información debe impedir el acceso no autorizado y 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. La identidad del informante sólo 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, y estos casos estarán sujetos a salvaguardas establecidas en la normativa aplicable.

Si la información recibida contuviera categorías especiales de datos personales, sujetos a protección especial, se procederá a su inmediata supresión, salvo que el tratamiento sea necesario por razones de un interés público esencial conforme a lo previsto en el artículo 9.2. g) del RGPD, según dispone el artículo 30.5 de la Ley 2/2023.

En todo caso, 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.

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 LOPDPGDD.

8. Planificación

8.1. Acciones para abordar riesgos y oportunidades

AUDRIA considera las políticas, procesos y funciones existentes, compras y contrataciones, comunicaciones, análisis de su contexto (DAFO), y las necesidades y expectativas de partes interesadas. Asimismo, determina los riesgos y oportunidades que deben abordarse para garantizar que el Sistema Interno de Información pueda lograr los resultados previstos, siendo estos:

- Fomentar y facilitar las comunicaciones.
- Apoyar y proteger a los informantes (incluyendo en su caso a otras partes interesadas relevantes que puedan estar de alguna manera involucradas).
- Asegurar que los reportes de irregularidades se traten de manera adecuada y oportuna;
- Mejorar la cultura organizacional y la gobernanza como consecuencia del buen funcionamiento del sistema de gestión y su promoción.
- Reducir los riesgos de irregularidades, siendo este sistema de gestión un importante "control a nivel entidad" con elevado poder disuasivo, preventivo y detectivo.
- Prevenir o reducir los efectos no deseados.
- Lograr la mejora continua (como una de las máximas aspiraciones del sistema de gestión).

En este sentido, AUDRIA ha planificado dos grupos de cuestiones:

1. Ha abordado los riegos derivados de las comunicaciones de las irregularidades y oportunidades.
2. Ha ideado los siguientes puntos:
   - Integrar e implementar acciones en sus procesos del Sistema Interno de Información
   - Evaluar la eficacia de estas acciones.
   - Involucrar al personal y a las partes interesadas pertinentes en la planificación del Sistema Interno de Información.
   - Proporcionar feedback al informante y a las partes interesadas.
   - Recopilar feedback del informante y otras partes interesantes pertinentes.

8.2. Objetivos del sistema de gestión de comunicaciones y planificación para alcanzarlos

La organización debería establecer los objetivos de su Sistema Interno de Información en las funciones y niveles pertinentes.

Los objetivos del sistema de gestión de comunicaciones deben:

a) Ser coherentes con la política
b) Ser medibles (si es factible)
c) Tener en cuenta los requisitos aplicables
d) Ser monitoreados
e) Ser evaluados
f) Ser comunicados
g) Ser actualizados y/o revisados según corresponda
h) Garantizar la detección temprana y la prevención de irregularidades

AUDRIA ha planificado como lograr los objetivos determinando:

OBJETIVO	ACCIÓN	RESPONSABLE	PLAZO
CONCIENCIACIÓN Y SENSIBILIZACIÓN	Realización de comunicados internos (mediante circulares) recordando la importancia y la existencia del Sistema Interno de Información.	Responsable del SII	Anualmente (2023 comunicación inicial; 2024 y 2025 comunicación de recordatorio).
	Realización de comunicados a través de la página web en el apartado de NOTICIAS, recordando la existencia del canal de información y del Sistema Interno de Información.	Responsable del SII	Comunicación inicial en diciembre 2023.
FORMACIÓN DEL PERSONAL	Formación específica del Sistema Interno de Información al personal de AUDRIA.	Responsable del SII	Enero 2024.
AUDITORIA INTERNA	Revisión del Sistema Interno de Información mediante la realización de una auditoría interna del SII.	Ángel Ortiz	Diciembre 2026.
PUBLICACIÓN Y DIFUSIÓN DEL SII	Publicación en la página web de la Política del Sistema Interno de Información.	Responsable del SII	30 de noviembre de 2023.
	Publicación en la página web del acceso al canal de denuncias.	Responsable del SII	30 de noviembre de 2023.
	Publicación en la página web del protocolo del canal de denuncias.	Responsable del SII	30 de noviembre de 2023.

9. Apoyo

En el presente apartado se definen los elementos para el apoyo, con la finalidad de conseguir los objetivos establecidos. Concretamente, dichos elementos, que afianzan el Sistema Interno de Información, son los siguientes:

- Asignación de recursos para el Sistema.
- Procurar las competencias del Responsable del Sistema.
- Cultivar la toma de conciencia sobre el Sistema.
- Desarrollar labores de comunicación interna y externa.

9.1. Recursos

El Sistema Interno de Información necesita de recursos materiales y humanos, correspondiendo al Órgano de Gobierno de AUDRIA determinarlos y facilitarlos.

A este efecto, AUDRIA se compromete a asegurar que el Sistema Interno de Información (en especial, el Responsable del Sistema) cuente con los recursos materiales y humanos necesarios para la gestión del canal de información de forma eficaz y proactiva, sin perjuicio de las responsabilidades que correspondan a otros órganos y, en su caso, a los órganos de administración y de dirección de AUDRIA.

Asimismo, AUDRIA se compromete a asignar las partidas presupuestarias necesarias para el Sistema Interno de Información, tanto partidas específicas y deliberadas como partidas por imprevistos o extraordinarias.

En la misma línea, en el caso de ser necesario y requerir la contratación de peritos, asesores externos u personal específico para realizar las investigaciones, AUDRIA deberá asegurar los recursos precisos para la contratación de tales expertos, previa autorización del Órgano de Gobierno.

9.2. Competencia del Responsable del Sistema

El término "competencia" significa la capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.

La competencia requiere de conocimientos, de experiencia y de habilidades para que una persona pueda realizar su función de forma eficaz. En este sentido, AUDRIA se compromete a proporcionar la formación e información necesaria al Responsable del SII designado, con el objetivo de que cuente con las competencias necesarias y suficientes para la gestión eficaz del Sistema y, en concreto, del canal de información.

9.3. Toma de conciencia y formación

La concienciación induce a un estado general de conocimiento sobre los aspectos generales del Sistema Interno de Información. En este sentido, AUDRIA se asegura de que cualquier persona, tanto interna como externa a la empresa, conozca el marco esencial del Sistema Interno de Información y sabe cómo debe comportarse y comunicar situaciones conflictivas.

La toma de conciencia no va dirigida a un público específico, sino a una pluralidad anónima de destinatarios.

Entre las diferentes acciones de concienciación que realiza AUDRIA, destacan las siguientes:

- Comunicados internos.
- Comunicados en la página web.
- Elementos informativos y formativos sobre el Sistema Interno de Información.

9.4. Comunicación

El principio de transparencia guarda relación con los comunicados y publicaciones de información del Sistema, tanto de forma interna como externa. Las comunicaciones no sólo permiten mantener informados a los diferentes colectivos, sino que también permiten poner en valor los cometidos de AUDRIA.

Siguiendo lo establecido en el artículo 25 de la Ley 2/2023, el canal de información debe ser fácilmente accesible para todas las personas potencialmente usuarias del canal y debe garantizar los mínimos de usabilidad que la Ley establece. Por este motivo, AUDRIA ha publicitado el uso y acceso del canal de información mediante:

- Publicación en la página web corporativa.
- Circular interna para el personal de la organización.
- Email informativo a los socios de AUDRIA.

AUDRIA debe determinar la necesidad de realizar comunicaciones internas y externas relevantes para la eficacia del Sistema que incluyan:

- El contenido de la comunicación.
- Cuándo comunicar.
- A quién comunicar.
- Cómo comunicar.
- Quién debe realizar la comunicación.
- Los idiomas y el lenguaje en el que deberá realizarse la comunicación.

10. Evaluación y revisión

10.1 Evaluación del desempeño

AUDRIA ha desarrollado un conjunto de indicadores medibles que ayudan a medir el logro de sus objetivos y a cuantificar el desempeño de su sistema, que son los siguientes:

- Recibir una comunicación en el canal de información relacionado con un acto ilícito o conducta contraria a la ética, moral y valores.
- Disminución del número de incidentes.
- Cantidad de tiempo utilizado para informar y tomar acciones correctivas ante incidentes ocasionados.
- Sanciones impuestas.
- Infracciones internas materializadas.
- Procedimientos administrativos abiertos
- Procesos judiciales abiertos
- Número de problemas no resueltos
- Tiempo del ciclo de investigación de cumplimiento (por tipo)
- Número de comunicaciones recibidas de forma errónea (fuera del ámbito objetivo o personal del Sistema).

El órgano encargado de determinar estos indicadores de desempeño es el Responsable del Sistema.

Los indicadores de desempeño se analizarán cada año.

10.2. Mantenimiento de registros

AUDRIA debe mantener actualizado un libro-registro de las informaciones recibidas y de las investigaciones internas que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad que establece la Ley 2/2023, de Protección a los Informantes.

El registro no será público, solamente por petición de la Autoridad judicial competente, por auto, y, a razón de un procedimiento judicial, podrá acceder a el registro.

Los datos personales se conservarán el tiempo necesario, y, en todo caso, no podrán conservarse por un periodo superior a 10 años.

10.3. Auditoría interna

El Sistema Interno de Información debe auditarse con el objetivo de someterse a un proceso sistemático, independiente, objetivo y documentado para constatar su adecuación.

Frecuencia de las auditorías internas

Trienal.

Requisitos del auditor interno.

AUDRIA tiene la posibilidad de externalizar la función de Auditoría Interna en una persona capacitada para ello. De esta forma, AUDRIA establece los siguientes requisitos mínimos que debe cumplir el auditor interno, cuando se externalice tal función:

- Experiencia en auditar Sistemas de Gestión (de Compliance, de PBC/FT, de cumplimiento normativo, etc.).
- Formación específica en Sistemas de Gestión (de Compliance, de PBC/FT, de cumplimiento normativo, etc.).

En todo caso, se requerirá la independencia del auditor en relación con la implantación del SII.

Método de designación del auditor interno.

AUDRIA procederá a documentar la comprobación de los requisitos del auditor, y se aprobará mediante Acta por el Órgano de Administración.

11. Aprobación del Sistema Interno de Información

El presente Sistema Interno de Información constituye una normativa interna para AUDRIA y, por ende, un elemento de alto nivel que debe ser aprobado por el Órgano de Gobierno.

El Órgano de Administración aprobó el Sistema Interno de Información mediante Acta de fecha 20 de noviembre de 2023, tratándose de la aprobación del manual del Sistema Interno de Información versión V.2023.1, la cual se determina que entre en vigor a partir del 1 de diciembre de 2023.

ANEXOS

ANEXO I - Matriz partes interesadas

MATRIZ DE PARTES INTERESADAS	
PARTE INTERESADA	**NECESIDADES Y EXPECTATIVAS**
CLIENTES	Mejora continua de los servicios prestados
	Derecho a comunicar / denunciar
	Minimización de los errores y la respuesta rápida ante incidencias
	Atención personalizada
	Mejorar las relaciones en el entorno de negocio
TRABAJADORES / PERSONAL	Formación adecuada
	Obligación y derecho de comunicar y de denunciar
	Crecimiento personal
	Seguridad en el trabajo
	Buen ambiente laboral
	Desarrollo profesional, igualdad y equidad laboral
SOCIOS	Derecho de comunicar y de denunciar
	Destinar recursos para la mejora del Sistema y del canal
ADMINISTRACIONES PÚBLICAS	Exigir que la organización cumpla con la normativa 2/2023 de Protección al denunciante y ofrecer la correspondiente protección en caso necesario.

ANEXO II – Formulario de comunicación del Responsable del SII a la AAI

Oficina Antifrau de Catalunya

Comunicació de responsable del sistema intern d'informació (art. 8 de la Llei 2/2023)

1 Dades de la comunicació

1.1 Tipus de comunicació

Indiqueu què és el que comuniqueu:

- ⊙ El nomenament de responsable del sistema intern d'informació (RSII)
- ○ El cessament de RSII
- ○ El cessament i nou nomenament de RSII

1.2 Dades del representant

El present formulari ha d'estar **signat** per una persona amb **poders de representació** de l'entitat comunicant. La signatura del formulari ha de fer-se amb un **certificat electrònic de representant** de l'entitat comunicant. S'admeten tots els certificats vàlids (idCAT, FNMT, etc.).

Si l'entitat pertany al **sector públic** i la persona que signa el formulari no disposa de certificat electrònic de representant, quan la representació **no** derivi d'una previsió legal caldrà **adjuntar l'acte o acord** en virtut del qual s'ostenta la representació de l'entitat.

Indiqueu les dades del representant de l'entitat comunicant que signa la present comunicació:

Nom	Carme
Cognom 1	Calbet
Cognom 2	Marce
NIF	46223540A
Condició	Apoderada

2 Dades de l'entitat comunicant

2.1 Dades de l'entitat

Indiqueu les dades generals de l'entitat:

Raó social	Audria Auditoria y Consultoria, S.L.P.
CIF	B65732141
Adreça física	Gran Via de les Corts Catalanes, 645, 6º 2ª
Adreça electrònica	https://www.audria.net/
Província	Barcelona
Localitat	Barcelona
Sector	Sector privat
Tipus d'ens públic	
Altres ens públics	
Tipus d'ens privat	altres formes societàries
Dependència (ens privat)	
Altres ens privats	
Òrgan designant	

2.2 Grup d'empreses (sector privat)

Indiqueu si l'entitat privada comunicant forma part d'un grup d'empreses (art. 11 de la Llei 2/2023):

⊙Sí O No

Si l'entitat comunicant forma part d'un grup d'empreses, **cal presentar una comunicació independent per cada empresa del grup**, encara que el RSII sigui comú a tot el grup.

Indiqueu la denominació o raó social i el CIF de l'empresa matriu o dominant del grup:

Raó social	**CIF**
Audria Auditors, S.L.P. (Andorra)	L-711296-R

Si l'entitat comunicant forma part d'un grup d'empreses, indiqueu si el RSII és comú a tot el grup (art. 11.2 de la Llei 2/2023):

⊙Sí O No

2.3 Obligació de disposar de sistema intern d'informació

Si l'entitat comunicant pertany al sector privat, indiqueu si està obligada a disposar d'un sistema intern d'informació (art. 10.1 de la Llei 2/2023):

⊙ Sí ○ No

Si heu contestat que sí a l'anterior apartat, indiqueu la causa de l'obligació de disposar d'un sistema intern d'informació (art. 10.1 de la Llei 2/2023):

Annexos I.B o II de la Directiva (UE) 2019/1937 (art. 10.1 b) de la Llei 2/2023)

2.4 Ens públics depenents i mitjans compartits en el sector públic

Indiqueu si l'entitat pública comunicant és depenent de o adscrita a alguna altra entitat pública:

○ Sí ⊙ No

Si l'entitat comunicant és depenent de o està adscrita a alguna altra entitat pública, **cal presentar una comunicació independent per cada entitat diferenciada**, encara que el sistema intern d'informació i, eventualment, el RSII sigui comú a les diferents entitats públiques vinculades.

Indiqueu la denominació o raó social i el CIF de l'entitat de capçalera de la qual depèn o a la qual està adscrita l'entitat comunicant:

Raó social	**CIF**

Indiqueu si l'entitat comunicant i l'entitat de capçalera de la qual depèn o a la qual està adscrita comparteixen el sistema intern d'informació (art. 14.2 de la Llei 2/2023):

○ Sí ⊙ No

Indiqueu si l'entitat comunicant comparteix el sistema intern d'informació amb una altra entitat pública de la qual **no** depèn ni a la qual està adscrita (art. 14.1 de la Llei 2/2023):

○ Sí ⊙ No

Si l'entitat comunicant comparteix el sistema intern d'informació amb altres entitats públiques, **cal presentar una comunicació independent per cada entitat diferenciada**.

Indiqueu la denominació o raó social i el CIF de l'entitat pública principal amb la qual l'entitat comunicant comparteix el sistema intern d'informació:

Raó social	**CIF**

3 Dades del nomenament o nou nomenament de RSII

Indiqueu en aquesta secció les dades del RSII (persona o òrgan col·legiat) que ha estat designat.

Si comuniqueu el cessament del RSII i el **nomenament d'un nou RSSI** (persona o òrgan col·legiat), indiqueu aquí les dades del nou RSII que ha estat designat.

En el cas de **canvi de tipus de RSII** —persona física a òrgan col·legiat o viceversa—, indiqueu en aquesta secció el tipus de RSII de nou nomenament i en la secció de cessament el tipus de RSII preexistent.

3.1 Tipus de RSII designat

Indiqueu quin tipus de RSII ha estat designat:

◉ persona física RSII
○ òrgan col·legiat RSII

3.2 RSII persona física

Indiqueu les dades de la persona física RSII designada:

Nom	Juan Luis
Cognom 1	Casanova
Cognom 2	Torreiro
NIF	36973522-X
Gènere	Home
Adreça electrònica	jlcasanova@audria.net
Telèfon	934515156

Si l'entitat comunicant pertany al **sector públic** indiqueu el tipus de vincle de la persona RSII amb l'entitat:

Si l'entitat comunicant pertany al **sector públic** indiqueu si la persona RSII desenvolupa simultàniament altres funcions o si les funcions de RSII s'han assignat a un càrrec preexistent:

○ Sí ◉ No

Si heu contestat que sí a l'anterior apartat, indiqueu les altres funcions que desenvolupa o el càrrec que ocupa la persona RSII:

Si l'entitat comunicant pertany al **sector privat** indiqueu si la persona RSII ocupa simultàniament un altre càrrec o si és el responsable de compliment normatiu (art. 8.5 i 8.6 de la Llei 2/2023):

- ○ La persona RSII no ocupa simultàniament cap altre càrrec
- ○ La persona RSII és la responsable de compliment normatiu
- ◉ La persona RSII ocupa simultàniament un altre càrrec

Si heu seleccionat la tercer de les anteriors opcions, indiqueu el càrrec que ocupa la persona RSII:

Conseller

Indiqueu la vigència de la designació de la persona RSII:

◉ Vigència indefinida ○ Vigència limitada fins:

Indiqueu si s'ha designat una persona física RSII substituta:

◉ Sí ○ No

Si heu contestat que sí a l'anterior apartat, indiqueu les dades de la persona física RSII substituta designada:

Nom	Josep Lluis
Cognom 1	Prims
Cognom 2	Vila
NIF	36976546-K
Gènere	Home
Adreça electrònica	lprims@audria.net
Telèfon	934515156
Càrrec	Soci

Si l'entitat comunicant pertany al **sector públic** indiqueu el tipus de vincle de la persona física RSII substituta amb l'entitat:

Indiqueu la vigència de la designació de la persona RSII substituta:

◉ Vigència indefinida ○ Vigència limitada fins:

3.3 RSII òrgan col·legiat

Indiqueu en la taula següent les dades de les persones que integren l'òrgan col·legiat RSII.

En el cas de **modificació parcial de la composició de l'òrgan col·legiat RSII** —cessament d'alguna o algunes de les persones que en formen part i nomenament de nous membres— indiqueu en la taula **només les dades dels nous membres de l'òrgan col·legiat RSII** que han estat designats i en la secció de cessament les dades dels membres cessats.

Nom	Cognom 1	Cognom 2	NIF	Gènere	Càrrec[1]	Adreça electrònica	Telèfon	Facultats de gestió	Substitut facultats de gestió	Vigència
								○ Sí	○ Sí	○ Indefinida ○ Fins:
								○ Sí	○ Sí	○ Indefinida ○ Fins:
								○ Sí	○ Sí	○ Indefinida ○ Fins:
								○ Sí	○ Sí	○ Indefinida ○ Fins:
								○ Sí	○ Sí	○ Indefinida ○ Fins:
								○ Sí	○ Sí	○ Indefinida ○ Fins:
								○ Sí	○ Sí	○ Indefinida ○ Fins:
								○ Sí	○ Sí	○ Indefinida ○ Fins:
								○ Sí	○ Sí	○ Indefinida ○ Fins:
								○ Sí	○ Sí	○ Indefinida ○ Fins:
								○ Sí	○ Sí	○ Indefinida ○ Fins:
								○ Sí	○ Sí	○ Indefinida ○ Fins:

[1] Si l'entitat comunicant pertany al **sector públic** indiqueu entre parèntesi, al costat del càrrec, el tipus de vincle amb l'entitat: funcionari, laboral, eventual, directiu, electe.

3.4 Acte o acord de designació

Indiqueu la data de l'acte o acord de designació:

Si l'entitat pertany al **sector públic** s'ha d'**adjuntar certificació de l'acte o acord** de designació de RSII. No obstant, si l'acte o acord de designació de RSII es troba publicat en el portal de transparència, indiqueu l'enllaç al document:

Si l'entitat pertany al **sector privat** l'aportació de certificació de l'acte o acord de designació de RSII és **potestativa**. No obstant, el present formulari té la condició de **declaració responsable** i, per tant, la persona signant declaració sota la seva responsabilitat que totes les dades consignades aquí relatives a la designació de RSII son certes. La declaració de dades falses en el present formulari comportarà l'exigència de les responsabilitats de qualsevol ordre legalment previstes.

4 Dades del cessament de RSII

Indiqueu en aquesta secció les dades del RSII (persona o òrgan col·legiat) que ha estat cessat.

En el cas de **canvi de tipus de RSII** —persona física a òrgan col·legiat o viceversa— indiqueu en aquesta secció el tipus de RSII preexistent que cessa i les dades corresponents.

4.1 Tipus de RSII cessat

Indiqueu quin tipus de RSII ha estat cessat:

O persona física RSII
O òrgan col·legiat RSII

4.2 RSII persona física

Indiqueu les dades de la persona física RSII cessada:

Nom	
Cognom 1	
Cognom 2	
NIF	

Indiqueu la causa del cessament de la persona RSII:

Si heu seleccionat "incompliment de les obligacions del càrrec de RSII" a l'anterior apartat, indiqueu breument en què han consistit els incompliments:

Si heu seleccionat "altres" a l'anterior apartat, indiqueu el breument el/s motiu/s del cessament:

Indiqueu si cessa la persona física RSII substituta:

○ Sí ○ No

Si heu contestat que sí a l'anterior apartat, indiqueu les dades de la persona física RSII substituta cessada:

Nom	
Cognom 1	
Cognom 2	
NIF	

Indiqueu la causa del cessament de la persona RSII substituta:

Si heu seleccionat "incompliment de les obligacions del càrrec de RSII" a l'anterior apartat, indiqueu breument en què han consistit els incompliments:

Si heu seleccionat "altres" a l'anterior apartat, indiqueu el breument el/s motiu/s del cessament:

4.3 RSII òrgan col·legiat

Indiqueu en la taula següent només les dades del/s membre/s cessat/s de l'òrgan col·legiat RSII.

Nom	Cognom 1	Cognom 2	NIF	Causa del cessament	Incompliments (si la causa és "incompliment obligacions del càrrec")	Altres causes cessament (si la causa és "altres")

4.4 Acte o acord de cessament

Indiqueu la data de l'acte o acord de cessament:

Si l'entitat pertany al **sector públic** s'ha d'**adjuntar certificació de l'acte o acord** de cessament de RSII. No obstant, si l'acte o acord de cessament de RSII es troba publicat en el portal de transparència, indiqueu l'enllaç al document:

Si l'entitat pertany al **sector privat** l'aportació de certificació de l'acte o acord de cessament de RSII és **potestativa**. No obstant, el present formulari té la condició de **declaració responsable** i, per tant, la persona signant declara sota la seva responsabilitat que totes les dades consignades aquí relatives al cessament de RSII son certes. La declaració de dades falses en el present formulari comportarà l'exigència de les responsabilitats de qualsevol ordre legalment previstes.

5 Informació relativa a comunicacions de l'OAC

Indiqueu si voleu rebre comunicacions o informació sobre activitats formatives o divulgatives de l'OAC relacionades amb les funcions de responsable del sistema intern d'informació

◉ Sí ○ No

Data i signatura

46223540A MARIA CARMEN CALBET (R: B65732141)

Firmado digitalmente por 46223540A MARIA CARMEN CALBET (R: B65732141)
Fecha: 2023.11.24 12:48:10 +01'00'

Oficina Antifrau de Catalunya

Informació relativa al tractament de les vostres dades personals

D'acord amb el Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'abril, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i la lliure circulació d'aquestes dades, la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, i la resta de normativa vigent en matèria de protecció de dades de caràcter personal, especialment les disposicions relatives a aquesta matèria de la Llei 2/2023, del 20 de febrer, reguladora de la protecció de les persones que informin sobre infraccions normatives i lluita contra la corrupció, quedeu informat/ada que:

1. El responsable del tractament de les vostres dades personals és la Direcció de l'Oficina Antifrau de Catalunya.

2. Les dades de contacte de la persona delegada de protecció de dades són delegadapd@antifrau.cat C/Ribes núm. 3, 08013-Barcelona, amb la qual podeu contactar per a totes les qüestions relatives al tractament de les vostres dades personals.

3. La finalitat del tractament de les vostres dades personals és la de mantenir un registre actualitzat de les persones designades o cessades com a responsables del sistema intern d'informació i del seu històric i vetllar pel compliment de les obligacions previstes a la Llei 2/2023, de 20 de febrer i la resta de normativa aplicable.

4. Pel que fa a la legitimació per al tractament de les vostres dades personals, aquest és un tractament és necessari pel compliment d'una missió en interès públic o en l'exercici de poders públics conferits al responsable del tractament (OAC) per la Llei 2/2023, de 20 de febrer (art. 8.3) d'acord amb l'atribució de funcions a l'OAC de la Llei 3/2023, del 16 de març. Quant al tractament relatiu a les comunicacions d'accions divulgatives en relació amb l'exercici de funcions de les persones responsables dels sistemes interns d'informació, aquest tractament es basa en el vostre consentiment (art. 6.1 a) de l'RGPD).

5. Sens perjudici que es puguin sol·licitar altres dades que no tenen la consideració de dada personal d'acord amb la normativa d'aplicació, les dades personals que seran objecte de tractament són les següents: dades personals de la persona representant, nom, cognoms i DNI de la persona responsable del sistema intern d'informació o de les persones que composen l'òrgan col·legiat (inclosa la indicació de la identitat de la persona delegada de l'òrgan), dades de les persones substitutes que s'hagin designat, si escau, dades de les persones representants, adreça, càrrec de la persona responsable del sistema, òrgan d'administració o de govern que l'ha designat, dades de contacte (telèfon, adreça electrònica), signatura manuscrita/electrònica, causes del cessament de les persones responsables del sistema; també les dades que puguin constar en l'acord de nomenament o cessament de la persona responsable del sistema (només entitats del sector públic de l'art. 13 de la Llei 2/2023, de 20 de febrer) i les que puguin constar en l'acreditació de la representació, si escau.

6. No es preveu la comunicació de les vostres dades, tret d'obligació legal.

7. Les vostres dades es tracten en el marc de l'activitat de tractament "Registre de les persones responsables dels sistemes interns d'informació" que consta al Registre d'activitats de tractament de l'OAC.

8. No està prevista la transferència internacional de les dades per a aquest tractament.

9. Les dades es conservaran per al temps indispensable per al compliment de la finalitat per a la qual es van recollir i fins després que s'hagi produït el cessament de la persona responsable del sistema intern d'informació només quan el tractament hagi deixat de ser necessari per a les eventuals responsabilitats que es poguessin determinar.

10. Podeu exercir els drets d'accés, rectificació, supressió, de limitació del tractament, de portabilitat de les dades i d'oposició d'acord amb el que preveuen els articles 15 i següents del Reglament (UE) 2016/679, del 27 d'abril mitjançant una comunicació adreçada a la Direcció de l'OAC a l'adreça electrònica bustiaoac@antifrau.cat o mitjançant els formularis que trobareu a la seu electrònica de l'OAC.

11. Podeu adreçar una reclamació adreçada a l'Autoritat Catalana de Protecció de Dades, especialment quan no hàgiu obtingut satisfacció en l'exercici dels vostres drets, mitjançant la seu electrònica de l'Autoritat (https://seu.apd.cat) o per mitjans no electrònics (per correu postal) adreçat a: c/Rosselló, 214, esc. A, 1r 1a, 08008 Barcelona o bé presencialment al Registre d'entrada de documents de l'APDCAT o al Registre d'entrada de qualsevol òrgan de l'Administració de la Generalitat de Catalunya o de l'Estat, o mitjançant la presentació de la reclamació en una oficina de correus d'acord amb la normativa d'aplicació.

Ribes 3
08013 Barcelona
T +34 935 545 555
bustiaoac@antifrau.cat
www.antifrau.cat

ANEXO III – Política del Sistema Interno de Información

1. OBJETO Y ALCANCE

La finalidad principal de la Política del Sistema Interno de Información, en lo sucesivo denominado "el Sistema" o "SII", es formalizar el compromiso de AUDRIA AUDITORÍA Y CONSULTORÍA, S.L.P., en adelante AUDRIA, con el cumplimiento de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción – en adelante Ley 2/2023 –. Además, establece los principios que guían tanto la responsabilidad de nuestra sociedad como los principios fundamentales de la normativa del SII, permitiendo a todas las partes interesadas informar sobre posibles irregularidades o acciones/omisiones contrarias a la Ley.

Esta política es aplicable a todas las partes interesadas en AUDRIA, incluyendo internamente a empleados, colaboradores, socios y directivos, y externamente a cualquier individuo que haya tenido algún tipo de vínculo con la entidad, incluyendo familiares de los empleados de AUDRIA.

2. PRINCIPIOS APLICABLES

La presente Política se basa en los siguientes principios:

a) **Exhaustividad, Integridad y Confidencialidad**. Todas las comunicaciones recibidas dentro del SII serán tratadas de manera trazable y segura, siguiendo las disposiciones de la Ley 2/2023 y el manual del SII, cumpliendo siempre con las leyes de protección de datos y derechos digitales.

Se garantizará la exhaustividad, integridad y confidencialidad de la información, la prohibición del acceso no autorizado, el almacenamiento duradero de la información, la protección integral del informante y el respeto a la buena fe.

b) **Independencia y Autonomía del Responsable del SII.** El Responsable del Sistema, inscrito debidamente en la Autoridad Independiente de Protección del Informante, no recibirá instrucciones de ningún superior dentro de la entidad, garantizando su independencia en el cumplimiento de las funciones del cargo.

c) **Objetividad e Imparcialidad en el examen de las informaciones recibidas.** Se evitarán los conflictos de interés, se respetará la presunción de inocencia y se asegurará el derecho a la defensa. Todas las actuaciones se llevarán a cabo con imparcialidad y de acuerdo con la legislación vigente.

d) **Transparencia y Accesibilidad**. Se asegurará el acceso al SII y a la herramienta de comunicación implementada en la entidad. La información será presentada de manera clara y fácilmente accesible, con suficiente publicidad sobre su uso, principios y garantías asociadas.

e) **Ausencia de represalias, Protección al informante y a otras partes involucradas**. Se protegerá a los informantes siempre que las comunicaciones sean realizadas de buena fe y de acuerdo con el SII y la Ley 2/2023, asegurando el compromiso con su protección.

f) **Confidencialidad y anonimato del informante**. El SII garantizará el anonimato y/o confidencialidad según elección del informante.

3. LIDERAZGO Y COMPROMISO

La sociedad asume la responsabilidad de garantizar que el SII funcione eficazmente. Además, se compromete a promover una cultura de cumplimiento adecuada.

4. RESPONSABLE DEL SISTEMA

El Responsable del Sistema es responsable de la operación del SII, incluyendo, entre otras acciones:

- Recibir las comunicaciones a través del canal de información designado.
- Iniciar procedimientos de investigación si son necesarios.
- Designar expertos externos en caso necesario.
- Garantizar el funcionamiento adecuado del canal de información.
- Informar anualmente al órgano de gobierno sobre las comunicaciones recibidas.

5. CANAL PÚBLICO

AUDRIA ha establecido un sistema público de comunicación de información para promover el cumplimiento de la Ley 2/2023. Este canal permite a los empleados, proveedores, clientes, colaboradores y otras partes interesadas reportar hechos o conductas ilícitas, o cualquier acción/omisión contraria a los objetivos y normas establecidas en el SII.

Este canal público, accesible a través del enlace

https://www.audria.net/canal-de-denuncias/ y cuyas pautas de uso están detalladas en el sitio web corporativo y en el manual del Sistema, garantiza la confidencialidad y/o anonimato según prefiera el informante.

6. INCUMPLIMIENTO SISTEMA INTERNO DE INFORMACIÓN

El incumplimiento de esta política puede conllevar a sanciones tanto para la organización como para las personas involucradas. Las sanciones pueden consistir en acciones disciplinarias como despidos, multas, e incluso el inicio de acciones legales civiles, administrativas o penales contra los individuos implicados, entre otros.

Cualquier individuo con conocimiento o sospecha de violación de esta Política debe informarlo a través del canal de información implementado en AUDRIA. La organización nunca tomará represalias contra personas que se nieguen a participar en acciones corruptas, incluso si esto ralentiza o impide cualquier tipo de negocio.

Las consecuencias del incumplimiento del Sistema Interno de Información se regirán según lo establecido en el convenio colectivo y el Estatuto de los Trabajadores, así como en otras leyes vigentes aplicables.

7. CONTROL, EVALUACIÓN Y REVISIÓN

El Responsable del Sistema supervisará la implementación, desarrollo y cumplimiento del Sistema Interno de Información. Evaluará periódicamente su eficacia y, en caso de infracciones importantes o cambios en la organización, estructura de control o actividad, se considerará su modificación.

Cada año el Responsable del Sistema revisará esta Política y propondrá modificaciones al Órgano de Administración para contribuir a su mejora continua, tomando en cuenta sugerencias de los profesionales de AUDRIA.

8. APROBACIÓN

La presente Política del Sistema Interno de Información ha sido aprobada por el Órgano de Administración de AUDRIA mediante Acta de fecha 20 de noviembre de 2023.

ANEXO IV - Protocolo del canal de comunicación

Versión V.2023.1

1. FINALIDAD

AUDRIA AUDITORÍA Y CONSULTORÍA, S.L.P., en adelante AUDRIA, con el objetivo de dar cumplimiento a su Sistema Interno de Información implementado – en adelante "el Sistema" o "SII" –, así como a la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre las infracciones normativas y de lucha contra la corrupción – en adelante Ley 2/2023 – ha procedido a instaurar un Canal de Información con el objetivo de que todas las personas físicas determinadas dentro del ámbito personal del citado SII puedan comunicar la existencia de incumplimientos o conductas contrarias a las normas contenidas dentro del ámbito material del SII de la organización.

En consecuencia, el objetivo del presente protocolo es regular el funcionamiento el Canal de Información, así como la gestión y tramitación de las comunicaciones que se reciban y de los procedimientos de investigación que deban ser iniciados, en su caso.

2. ÁMBITO DE APLICACIÓN

Ámbito material

El Canal de Información habilitado en AUDRIA permite las comunicaciones en relación a las materias que a continuación se describen, en cumplimiento de la Ley 2/2023, así como, también, de la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, por tener la consideración de sujeto obligado a esta Ley.

a) Ley 2/2023:
   - Acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea, siempre que:

     1. Entren dentro del ámbito de aplicación 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;
     2. 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);

3. 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.

- Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave.
- Infracciones del Derecho laboral en materia de seguridad y salud en el trabajo.

b) Ley 10/2010:
   - Cualquier infracción de las disposiciones contenidas en la Ley vigente de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo.

c) Prevención del acoso sexual y por razón de sexo:
   - Cualquier actuación contraria a la normativa vigente en materia de acoso sexual y por razón de sexo (Ley Orgánica 3/2007, para la igualdad efectiva de mujeres y hombres, artículo 48) , así como a lo dispuesto en el Protocolo de prevención y abordaje del acoso sexual y por razón de sexo de AUDRIA.

Ámbito personal

La protección contenida en la Ley 2/2023, así como la regulación del presente porotcolo, es de aplicación a los siguientes informantes:

1. *Informantes que trabajen en el sector privado o público y que hayan obtenido información sobre infracciones en un contexto laboral o profesional, comprendiendo en todo caso:*
   a. *las personas que tengan la condición de empleados públicos o trabajadores por cuenta ajena;*
   b. *los autónomos;*
   c. *los accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa, incluidos los miembros no ejecutivos;*
   d. *cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.*
2. *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. *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.*

3. FORMAS DE INFORMAR PERMITIDAS

AUDRIA ha establecido, en consonancia con la Ley 2/2023, las siguientes formas de informar:

- Canal interno (de carácter público): mediante la herramienta informática on-line denominada "Ovet-Auki". Gestión externalizada.
- Canal externo: Autoridad Independiente de Protección al Informante.
- Revelación pública
- Correo postal. Gestión interna.
- Entrevista presencial. Gestión interna.
- Telefónico. Gestión interna.

CANAL INTERNO

AUDRIA a instaurado una herramienta informática on-line, denominada "OVET AUKI" mediante la cual cualquier persona puede acceder a través del siguiente enlace: https://www.ovetauki.com/index.php?route=login/complaint&c_key=cexJzyREKMqqzuuBRjhAWVDWFQcjyAtoYnCp.

Este canal, cuya gestión está externalizada a los expertos de TARINAS VILADRICH ADVOCATS I PROCURADORS, SLP, permite tanto las comunicaciones anónimas como las confidenciales, a elección del informante.

Funcionamiento y características

El acceso al canal de información se realiza mediante el enlace https://www.ovetauki.com/index.php?route=login/complaint&c_key=cexJzyREKMqqzuuBRjhAWVDWFQcjyAtoYnCp, desde cualquier dispositivo y a cualquier hora del día, los 365 días del año.

El informante, deberá ir cumplimentando las distintas fases de confección de la comunicación, siguiendo las instrucciones dadas por la propia plataforma, y debiendo describir los hechos de la forma más detallada posible, asi como adjuntar todas las pruebas que se disponga, siempre con el objetivo de facilitar el posterior procedimiento de investigación, en su caso.

Se puede consultar el Manual de uso del canal de información OVET AUKI, adjunto como **Anexo IV.3** del presente Protocolo.

En la última fase de la comunicación, el informante deberá elegir, expresamente, si desea que la comunicación realizada tenga un carácter confidencial y, por lo tanto, que se conozca su identidad o, por el contrario, que tenga un carácter anónimo. En el caso de que se elija la opción de carácter anónimo, el informante deberá conservar el código de comunicación generado para poder acceder con posterioridad a la plataforma OVET AUKI y así poder consultar el estado de la comunicación, ponerse en contacto con los gestores del canal o con la organización, etc.

Todo ello, viene debidamente detallado en el Manual de uso del canal de información OVET AUKI.

En caso de dudas o incidencias, pueden dirigirse a los técnicos de la plataforma mediante el correo electrónico soporte@ovetauki.com

CANAL EXTERNO

Cualquier persona física podrá informar ante la Autoridad Independiente de Protección al Informante correspondiente, siendo la Oficina Antifraude de Cataluña, a través del siguiente enlace: https://antifrau.cat/es/18-investigacio/1123-bustia-de-denuncies-anonimes-2.html

REVELACIÓN PÚBLICA

Se entenderá revelación pública la puesta a disposición del público de información sobre acciones u omisiones previstas en el artículo 2 de la Ley 2/2023.

Se protegerá a las personas siempre cuando cumpla **alguna** de las siguientes condiciones:

a) Que previamente a la revelación pública haya realizado una comunicación mediante los canales anteriores (interno, público y/o externo), sin medidas apropiadas en el plazo máximo establecido (3 meses).
b) Que haya motivos razonables para pensar que, o bien la infracción puede constituir un peligro inminente o manifiesto por el interés público, en particular cuando se dé una situación de emergencia, o exista un riesgo de daños irreversibles, incluido un peligro para la integridad física de una persona; o bien, en caso de comunicación a través del canal externo de información, exista riesgo de represalias o haya pocas probabilidades de que se dé un tratamiento afectivo a la información debido a las circunstancias particulares del caso, tales como la ocultación destrucción de pruebas, la connivencia de una autoridad con el autor de a infracción, o que esté implicada en la infracción.

Las condiciones para acogerse a la protección prevista en el apartado anterior no son exigibles cuando la persona haya revelado información directamente a la prensa de acuerdo con el ejercicio de la libertad de expresión y de información veraz previstas constitucionalmente y en la legislación de desarrollo.

Correo postal

Se podrán enviar comunicaciones por escrito a través del correo postal a la siguiente dirección:

AUDRIA AUDITORÍA Y CONSULTORÍA, S.L.P.

A la atención del Sr. Juan Luis Casanova

(Responsable del Sistema Interno de Información)

Gran Vía de les Corts Catalanes, 645, 6º 2ª – 08010 - Barcelona

Todas las comunicaciones recibidas por correo postal se tratarán garantizando los derechos del informante y la confidencialidad, en el caso de proporcionar una vía de comunicación con el informante se utilizará para notificar el curso de la comunicación o para cualquier otro trámite o cuestión necesaria.

Entrevista presencial

Se habilita la opción de poder comunicar presencialmente con el Responsable del Sistema dentro del plazo máximo de 7 días.

Se garantiza la protección de los datos según el Reglamento (UE) 2016/679 y la Ley 3/2018 de Protección de datos Personales y garantía de los derechos digitales, en el momento de transcribir la comunicación.

4. TRATAMIENTO DE LA COMUNICACIÓN

El presente apartado aplica a las comunicaciones recibidas en la organización.

El procedimiento de investigación de las comunicaciones recibidas en la Autoridad Independiente de Protección al Informante queda supeditado al Estatuto de la citada autoridad.

Contenido mínimo de la comunicación

El informante tiene el deber de proporcionar toda la información lo más detallada posible, así como de proporcionar todos los datos y pruebas que disponga, con el fin de facilitar el posible procedimiento de investigación posterior. Asimismo, a fin de poder llevar a cabo dicho procedimiento de investigación, se exige que la comunicación disponga de, como mínimo, la siguiente información:

- Descripción de los hechos.
- Los indicios sobre los que se basa la sospecha del informante.
- Si se conoce, la identidad de la/s persona/s que ha/n realizado los hechos, o de aquellas personas que hayan podido encubrirlo.
- Si se conoce, lugar donde han ocurrido los hechos.

- Fecha de cuando ha tenido conocimiento de los hechos, o desde cuando está teniendo conocimiento el informante.
- Cómo ha conocido los hechos el informante (si lo ha presenciado personalmente, a través de terceros, mediante pruebas documentales, etc.).

Procedimiento de recepción, seguimiento e investigación de la comunicación.

Acuse de recibo o justificante de recepción

El informante deberá recibir el acuse de recibo o justificante de recepción de la comunicación en el plazo máximo de 7 días naturales desde su envío.

Lo anterior, aplica en todos los casos de las comunicaciones realizadas a través de la plataforma OVET AUKI y, en los demás casos, en aquellas comunicaciones en las que el informante haya proporcionado un método de contacto.

Filtraje de las comunicaciones recibidas

Los gestores externos del canal de información serán los encargados de realizas el primer filtraje de la comunicación recibida, con el fin de valorar si (i) el informante se encuentra dentro del ámbito personal del Sistema Interno de Información de AUDRIA y (ii) si la comunicación se encuentra dentro del ámbito material del citado Sistema. En el caso de las comunicaciones anónimas, solamente se filtrará teniendo en cuenta el ámbito material, al hacerse imposible la identificación del informante.

Una vez realizado el primer filtraje, se procederá a:

a) En el caso de NO encontrarse dentro del ámbito personal y/o material del SII, se archivará la comunicación recibida, se generará un informe que justifique el motivo por el cual se ha procedido al archivo, y se notificará al informante, proporcionándole una copia del informe justificativo en cuestión.
b) En el caso de SÍ encontrarse dentro del ámbito personal y/o material del SII, se procederá a comprobar si la comunicación cuenta con el contenido mínimo antes mencionado. En el caso que falte información para proseguir, se procederá a ponerse en contacto con el informante con el objetivo de que, en un plazo máximo de 15 días, proporcione la información faltante.
    i. En el caso que el informante no proporcione la información faltante, se procederá al archivo de la comunicación y a la correspondiente notificación y entrega del informe justificativo de archivo, sin perjuicio que el informante pueda realizar una nueva comunicación sobre el mismo hecho.
    ii. En el caso que el informante haya utilizado un método distinto al portal OVET AUKI y no haya proporcionado un método de contacto, se procederá a la incoación del procedimiento de investigación, dejando constancia de lo sucedido y del posible archivo de la comunicación por no contar con información suficiente para llevar a cabo un proceso de investigación con todas las garantías.

d) En el caso de SÍ encontrarse dentro del ámbito personal y/o material del SII y de que la comunicación cuente con el contenido mínimo exigido, se tendrá que comprobar que los hechos descritos en el contenido de la comunicación no se encuentren siendo ya investigados o que ya hayan sido investigados, y que el informante no aporte pruebas o información nueva que motiven la incoación de un nuevo procedimiento de investigación:
   i. En el caso que los hechos ya hayan sido investigados o estén siendo investigados, y el informante NO aporte pruebas o información nueva, se procederá al archivo de la comunicación con informe justificativo que lo motive.
   ii. En el caso que los hechos ya hayan sido investigados o estén siendo investigados, y el informante SÍ aporte pruebas o información nueva, se procederá a la incoación de un nuevo procedimiento de investigación, que se llevará a cabo junto con la información y/o procedimiento de investigación que se haya llevado o se esté llevando a cabo por los mismos hechos descritos en la comunicación.
   iii. En el caso que los hechos no hayan sido nunca investigados, se procederá a la incoación del procedimiento de investigación.

e) En el caso de SÍ encontrarse dentro del ámbito personal y/o material del SII y que la comunicación cuente con el contenido mínimo exigido, y no se trate de una causa que ya ha sido o está siendo investigada, los gestores externos del canal, en el caso de la plataforma OVET AUKI, remitirán la comunicación recibida al Responsable del SII para que éste proceda, a la mayor brevedad posible, a incoar el correspondiente procedimiento de investigación. En el caso de haber recibido la comunicación por otros medios, la comunicación es recibida desde un primer momento por el propio Responsable del SII.

Procedimiento de investigación

Incoación del expediente

La persona que debe proceder a la incoación del procedimiento de investigación es el Responsable del SII, mediante Acta de inicio del procedimiento de investigación, en la que se deberá adjuntar la información contenida en la comunicación recibida. En la misma Acta, se deberá detallar los motivos por los cuales se admite la comunicación a trámite, y el nivel de verosimilitud que desprende, así como si se considera que se ha realizado, o no, de buena fe.

Asimismo, se deberá analizar la capacidad propia del Responsable del SII para llevar a cabo el procedimiento de investigación o, en su caso, la necesidad de contar con otras personas de la organización o con personas externas expertas, siempre siguiendo el procedimiento que se especifica más adelante en este protocolo, y respetando todas las garantías y la confidencialidad máxima de la comunicación recibida y del informante. De igual forma, en caso de ser necesario, el Responsable del SII puede designar a un instructora del procedimiento de investigación distinto a ella, ya sea de la propia organización o un externo, siempre respetando las garantías y la confidencialidad.

Por otro lado, se deberán establecer los procedimientos de investigación que permitan la preservación de pruebas y el respeto a los derechos de los trabajadores. Estas actuaciones pueden incluir entrevistas de índole personal con departamentos específicos de la organización o personas implicadas en los hechos comunicados. También se podrá requerir de un profesional para peritar los daños y el delito, siguiendo el procedimiento de invitación de externos que se describe más adelante.

Del mismo modo, se deberá establecer los departamentos o áreas que deberán estar informados de la presente investigación y a qué nivel jerárquico, dependiendo de: (i) el nivel jerárquico y número de posibles personas implicadas y (ii) a necesidad de involucrar a otros departamentos.

Finalmente, se deberá valorar la necesidad de informar al órgano de gobierno de la organización sobre la investigación realizada, dependiendo si éste puede verse involucrado en el proceso o poder llevar posibles represalias que, en todo caso, se deben evitar.

Plazo máximo de resolución

El plazo máximo de resolución del procedimiento de investigación, contando a partir de la notificación de recepción de la comunicación, son los siguientes:

- Para las comunicaciones recibidas en materia de la protección de los derechos de la Unión Europea (Ley 2/2023): 90 días naturales.
- Para las comunicaciones recibidas en materia de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo (Ley 10/2010): 90 días naturales.
- Para las comunicaciones recibidas en materia de acoso sexual o por razón de sexo (Ley Orgánica 3/2007, para la igualdad efectiva de mujeres y hombres y, en concreto, según el protocolo para la prevención y actuación al acoso sexual y acoso por razón de sexo en el ámbito laboral del Ministerio de Igualdad de España, elaborado por la Subdirección General para el Emprendimiento, la Igualdad en la Empresa y la Negociación Colectiva, de octubre de 2021): 10 días hábiles.

Solamente en aquellos casos en que se pueda justificar, de forma expresa, por escrito y de forma motivada, la complejidad de la investigación, se podrá extender el plazo por 90 días naturales más.

Invitación de personas externas al procedimiento de investigación

Como se ha comentado anteriormente, el Responsable del SII deberá analizar la comunicación recibida y justificar si se deben invitar personas externas al procedimiento de investigación para asegurar su éxito. Alguno de los motivos por los que se pueden invitar a personas externas, pueden ser:

- Falta de conocimientos específicos o técnicos sobre los hechos comunicados.
- Posible conflicto de interés por parte del Responsable del SII.
- Estrategia en el momento de recopilar pruebas para la investigación, por ejemplo, en el momento de realizar entrevistas al personal es posible que una persona externa pueda obtener más información que una interna.

Para invitar a personas externas al procedimiento de investigación, el Responsable del SII deberá levantar Acta justificando los motivos, y la/s persona/s externa/s deberán firmar la declaración de ausencia de conflictos de intereses – adjunta al presente protocolo como Anexo IV.1 – y el correspondiente acuerdo de confidencialidad – adjunto al presente protocolo como Anexo IV.2 –.

Resolución del expediente y notificación

Finalizado el procedimiento de investigación, el Responsable del SII deberá:

1. Realizar un informe del procedimiento de investigación llevado a cabo, desarrollando todas las fases y las pruebas recopiladas, así como los posibles incidentes que hayan podido haber y su resolución.
2. Levantar Acta de cierre del procedimiento de investigación, especificando la resolución tomada.

Las posibles resoluciones que puede tener el procedimiento de investigación, son las siguientes:

a) Archivo de la comunicación.

Se puede dar el archivo de la comunicación, después de haber realizado el procedimiento de investigación, por numerosos motivos, por ejemplo:

- No contar con suficiente información o pruebas para seguir investigando.
- Necesitar la colaboración del informante para poder llevar a cabo la investigación y que éste se niegue.
- Que el resultado de la investigación sea que los hechos descritos realmente no sucedieron, o que no se trate de una conducta contraria a las normas o legislación vigente, o a las políticas implementadas en la organización.

b) Elevación de la comunicación a la autoridad competente.

En aquellos casos en que se haya podido comprobar que se trata de hechos, verosímiles, que puedan constituir cualquier clase de delito tipificado en el Código Penal español vigente, se deberá elevar la comunicación de forma inmediata al Ministerio Fiscal.

De igual forma, en aquellos casos en que el Responsable del SII lo considere pertinente, deberá elevar la comunicación a la autoridad competente.

c) Resolución interna de la comunicación, con o sin sanción.

En aquellos casos en que se pruebe que los hechos de la comunicación efectivamente han ocurrido, se deberá proceder a aplicar solución. Puede ser que no sean constitutivos de actos ilícitos o que se trate de conductas leves, procediendo a su resolución inmediata. En el caso de que no se pueda aplicar una resolución inmediata, se deberá planificar la misma, determinando un plazo concreto para ello y desarrollando la solución que se aplicará. De igual forma, se deberá valorar la posible sanción a la/s persona/s que hayan realizado los hechos objeto de sanción, todo ello de forma motivada y expresa.

5. DERECHOS Y OBLIGACIONES

Se deberá informar de buena fe y se garantizará que el informante no sea objeto de represalias. Asimismo, con la finalidad de asegurar que ninguna persona que informe de buena fe un hecho presuntamente ilícito sea objeto de represalias, todas las comunicaciones irán siempre dirigidas al Responsable del Sistema. No obstante, en caso de que la persona objeto de la comunicación sea el propio Responsable del Sistema, la comunicación se podrá dirigir a **Don Lluis Prims Vilà- Director**, quien asumirá el rol de Responsable del SII solamente por lo que refiere al procedimiento de investigación de la comunicación en cuestión, debiendo respetar todo lo establecido en el presente protocolo.

La identidad del informante permanecerá anónima o confidencial, a elección del informante, o a excepción de consentimiento por parte de este para dar a conocer su identidad. Asimismo, la identidad del informante, en todo caso, se tratará de forma confidencial. En este sentido, el Responsable del Sistema no facilitará la identidad del informante bajo ningún concepto exceptuando – en caso absolutamente imprescindible – a las personas externas (o internas) que puedan formar parte del procedimiento de investigación debiendo, previamente, firmar el correspondiente acuerdo de confidencialidad anexo al presente protocolo.

Asimismo, la identidad del informante podrá ser revelada por requerimiento judicial, proporcionando la identidad al Juez, Fiscal, Policía o autoridad administrativa competente para que traslade el resultado de la investigación realizada.

La/s persona/s objeto de la comunicación recibida – es decir, la/s persona/s a la/s que se le/s atribuye los hechos descritos en la comunicación – podrá/n ejercer el derecho de acceso, no estando incluido en el citado derecho la revelación de datos de identificación del informante.

No se sancionará ni se tomará represalias contra una persona por formular una comunicación, siempre que se haya realizado de buena fe.

6. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

La Ley 2/2023, en su Título VI, establece las directrices del tratamiento de los datos latos personales que se derivan de la aplicación de Ley 2/2023, siendo que dicho tratamiento de los datos se regirá 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. Esto es: informar sobre el tratamiento de los datos y el ejercicio de derechos, la licitud del tratamiento, Asimismo, nadie obtendrá datos que permita identificar al informante y se deberá contar con las medidas técnicas y organizativas necesarias para preservar la identidad y garantizar la confidencialidad y/o anonimato, en su caso, de los datos de las personas afectadas.

Por otro lado, en el artículo 32 se recoge el tratamiento de datos personales en el Sistema Interno de Información, concretamente hay que tener en cuenta que el acceso a los datos del Sistema Interno de Información queda limitado según las responsabilidades y competencias 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 de la entidad u organismo, 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.

Finalmente, se deberá incluir en el Registro de Actividad de Tratamiento conforme lo establecido en el artículo 30 de la RGPD.

Responsable del Tratamiento:

DENOMINACIÓN SOCIAL	**AUDRIA AUDITORÍA Y CONSULTORÍA, S.L.P.**
NIF	B65732141
UBICACIÓN	Gran Vía de les Corts Catalanes, 645, 6º 2ª – 08010 - Barcelona

Finalidad. Gestionar los datos del interesado con el fin de poder tramitar y gestionar la denuncia interpuesta mediante el canal habilitado,

Legitimación.

- El tratamiento de datos personales, cuando sea obligatorio disponer de un Sistema Interno de Información y en los supuestos de comunicación interna, se entenderá lícito el tratamiento en virtud de lo que disponen los artículos 6.1.c) del RGPD, el artículo 8 de la LOPDGDD, y 11 de la Ley Orgánica 7/2021, de 26 de mayo.
- El tratamiento de datos personales en los supuestos de canales de comunicación externos se entenderá lícito en virtud de lo que disponen los artículos 6.1.c) del RGPD.
- El tratamiento de datos personales derivado de una revelación pública se presumirá amparado en lo dispuesto en los artículos 6.1.e) del RGPD.
- En el supuesto que se trataran categorías especiales de datos personales por razones de un interés público esencial, el tratamiento será lícito conforme a lo previsto en el artículo 9.2.g) del RGPD.

Transferencias Internacionales de Datos. No se realizan Transferencia Internacionales de datos a terceros países fuera de la Unión Europea.

Comunicación 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.

Conservación de Datos. 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. 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.

Derechos de los interesados. El interesado que podrá ejercer los derechos de acceso, rectificación y supresión (Derecho al olvido), limitación de los datos, portabilidad de los datos y oposición, enviando un escrito a **Juan Luis Casanova**, así como, presentar una reclamación ante la Autoridad de Control competente en materia de protección de datos (en la actualidad la Agencia Española de Protección de Datos) en el supuesto que no obtenga una respuesta satisfactoria y desee formular una reclamación u obtener más información al respecto de cualquier de estos derechos.

7. COMUNICACIÓN Y FORMACIÓN

Para poder garantizar los derechos de los destinatarios del presente protocolo, así como que los mismos conozcan sus obligaciones, se debe proveer información previa, precisa e inequívoca a los miembros de AUDRIA sobre la existencia este protocolo.

Se establece la obligación de informar de la existencia y acceso al canal de información mediante, como mínimo, la publicación en la página web.

El Responsable del Sistema deberá coordinar y controlar las acciones de comunicación y formación necesarias para asegurar que todas las personas que tienen relación con AUDRIA conozcan su existencia y su forma de operar.

8. APROBACIÓN, ENTRADA EN VIGOR Y REVISIÓN

El Órgano de Gobierno de AUDRIA aprueba el presente protocolo del Canal de Información, siendo la Versión V.2023.1 mediante Acta de fecha 20 de noviembre de 2023.

Anexo IV.1 - DECLARACIÓN DE AUSENCIA DE CONFLICTOS DE INTERESES (DACI)

El Responsable del Sistema Interno de Información de AUDRIA, como instructora del procedimiento de investigación de la comunicación recibida con número de expediente XXXXXXXX y código de comunicación XXXXXXX, invita a XXXXXXX, mayor de edad, con DNI nº XXXXXXXXXXX a formar parte del proceso de investigación citado por los siguientes motivos:

Xxxxx

xxxxx

Don/Doña xxxxxxxxxxxxxxxxx, habiendo sido informado de la invitación y de los hechos del caso, declara:

Primero. Estar informado de lo siguiente:

Que el artículo 61.3 «Conflicto de intereses», del Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo, de 18 de julio (Reglamento financiero de la UE) establece que «existirá conflicto de intereses cuando el ejercicio imparcial y objetivo de las funciones se vea comprometido por razones familiares, afectivas, de afinidad política o nacional, de interés económico o por cualquier motivo directo o indirecto de interés personal.»

Segundo. Que no se encuentra incurso en ninguna situación que se pueda calificar de conflicto de intereses, en relación con las actuaciones que derivan de sus funciones, así como en relación con el propio cargo que ocupa en AUDRIA, como:

- Tener interés personal en el asunto de que se trate o en otro en cuya resolución pueda influir la de aquél; ser administrador de sociedad o entidad interesada, o tener cuestión litigiosa pendiente con el Órgano de Gobierno, o cualquier otro interesado en el asunto de que se trate.
- Tener vínculo matrimonial o situación de hecho asimilable y el parentesco de consanguinidad dentro del cuarto grado o de afinidad dentro del segundo, con el Órgano de Gobierno, o cualquier otro interesado en el asunto de que se trate.
- Tener amistad íntima o enemistad manifiesta con alguna de las personas mencionadas en el apartado anterior.

Tercero. Que su función como "xxxxxxxx" con las siguientes responsabilidades atribuidas:

xxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxx

No dificulta, ni entorpece en modo alguno, la resolución a la investigación abierta ni interfiere negativamente al respecto.

Cuarto. Que, en caso de darse alguna situación de conflicto de interés, ya sea en general por las funciones y el cargo que está ejerciendo, como en particular por alguna actuación en concreto, se compromete a poner en conocimiento del Responsable del Sistema, sin dilación, cualquier situación de conflicto de intereses que se dé o pudiera dar lugar. En concreto, se compromete a poner en conocimiento de la citada responsable, de manera expresa:

- Si, en su conocimiento, existe un conflicto de intereses aparente, potencial o real vinculado al cargo.
- Si hay circunstancias que lo pudieran llevar a una situación de conflicto de intereses aparente, potencial o real en un futuro cercano.

Quinto. Que conoce que una declaración de ausencia de conflicto de intereses que se demuestre que sea falsa, comportará las consecuencias disciplinarias/administrativas/judiciales que establezca la normativa aplicable vigente en ese momento.

Y por la presente, firma en fecha xxx de xxx de 202x.

xxxxxxxxxxxxx

Anexo IV.2 - ACUERDO DE CONFIDENCIALIDAD

De una parte, [entidad], con domicilio [dirección], y, provista de Número de Identificación Fiscal (NIF) [número], representada en este acto por [responsable SII] mayor de edad, con DNI [indicar] (en adelante "Parte Emisora")

Y, de otra parte, [indicar], con domicilio en [indicar] y, provista de Número de Identificación Fiscal (NIF) [indicar] representada en este acto por [indicar] mayor de edad, con DNI [indicar], (en adelante "Parte Receptora")

Se reconocen ambas Partes con capacidad legal suficiente y poder bastante para este acto y, a tal efecto

EXPONEN:

I. Que, la "Parte Emisora" desea intercambiar con la "Parte Receptora" información necesaria para el proceso de investigación número xxxxxxxxx de la comunicación con código: xxxxxxxxxxxx.

II. Que, para prestar los servicios indicados en el Exponen I, implica que la "Parte Receptora" accede a información confidencial de la "Parte emisora", así como, a datos de carácter personal, siendo ésta la entidad Responsable del Tratamiento.

III. Que, con el fin de mantener confidencial la información proporcionada por la "Parte Emisora" así como para dar cumplimiento a la normativa vigente en materia de protección de datos de carácter personal, constituye la voluntad de las partes proceder a regular las condiciones relativas a la confidencialidad de la información y el tratamiento de los datos personales.

IV. A los efectos del presente acuerdo, se entenderá por "Información Confidencial" enumerando a título enunciativo que no limitativo, las comunicaciones, registros, datos, apuntes, documentos, planos, briefings, maquetas, información general de la "Parte Emisora" o de la relación de ésta con otros clientes o proveedores, datos de personal, procesos y procedimientos relacionados con cualquier actividad desarrollada, así como el know-how o cualquier tipo de información técnica, operativa y comercial de todo tipo, planos, investigaciones, equipamientos, informes, previsiones, precios, costes, especificaciones, documentos, estén o no sujetos o protegidos por derechos de autor, patentes, marcas registradas, secretos comerciales, etc., que se encuentren o no registrados, y que hayan sido revelados o comunicados de cualquier forma (verbal, escrita o por soporte magnético o cualquier otro medio telemático o electrónico, etc.) con anterioridad o posterioridad a la fecha del presente acuerdo; así como cualquier dato o información relacionada con la actividad empresarial de la *"Parte Emisora"*, ya sea de carácter financiero, contable, laboral, económico, comercial, y/o industrial.

Las obligaciones de confidencialidad exigibles a la "Parte Receptora" no se aplicarán a aquella información que:

a. Sea o se convierta en información de dominio público a través de una fuente debidamente legitimada para divulgar la Información Confidencial, o
b. La "Parte Emisora" haya autorizado previamente su divulgación expresamente o por escrito, o
c. Sea recibida por la "Parte Receptora" por parte de un tercero legalmente facultado para difundirla, sin infringir ninguna obligación frente la "Parte Emisora" ni derecho alguno de ésta, y que no esté sujeta a un acuerdo de confidencialidad entre las partes, o

d. Aquella cuya divulgación le sea requerida a la "Parte Receptora" por una orden judicial o cualquier entidad de carácter público con potestad suficiente para ello, en cuyo caso, con anterioridad a la divulgación, la "Parte Receptora" deberá informar de inmediato a la "Parte Emisora" sobre tal circunstancia enviándole por conducto fehaciente una copia del requerimiento recibido, debiendo informar a la "Parte Emisora" en cuanto a la forma de cumplir con el requerimiento recibido y el contenido y alcance de la divulgación, procurando la "Parte Receptora" cooperar en todo cuanto esté a su alcance para asegurar el mantenimiento del carácter confidencial de la información confidencial, cuidando en cualquier caso que el contenido y el acceso por terceras personas a la misma sea lo más restringido posible.

V. Que, como consecuencia de lo anterior, ambas partes, reconociéndose mutuamente capacidad suficiente para contratar y obligarse, acuerdan la celebración del presente contrato, que quedará sujeto a las siguientes

CLÁUSULAS:

PRIMERA. - Responsabilidades:

La "Parte Receptora" se compromete a:

- Utilizar la Información Confidencial de forma reservada.
- Restringir el acceso a la Información Confidencial a sus respectivos empleados, asociados, subcontratados y a cualquier persona que, por su relación con las Partes, pueda o deba tener acceso a dicha información, advirtiendo de dicho deber de confidencialidad.
- La Información Confidencial sólo podrá ser utilizada por la otra cuando así sea necesario para el desarrollo de los Servicios y a los exclusivos efectos del cumplimiento del objeto del mismo.

- Proteger la Información Confidencial utilizando los mismos medios de protección que utiliza para proteger su propia Información Confidencial. El acceso a dicha información quedará restringido sólo a aquellos empleados de la "Parte Receptora" que deban conocerla para cumplir con el objeto del presente Acuerdo.
- No reproducir ni copiar la Información Confidencial a menos que se obtenga el consentimiento previo y escrito de la parte que la haya dado a conocer.
- Devolver a la "Parte emisora", todos los documentos que contengan información confidencial y todas las copias de esos documentos cuando les sean requeridos. Toda Información Confidencial, papeles, libros, cuentas, grabaciones, listas de clientes y/o socios, programas de ordenador, procedimientos, documentos de todo tipo o tecnología con independencia del soporte que la contuviera, tendrá el tratamiento de secreto, confidencial y restringido. En todo lo referente a este acuerdo el término "documento" incluye discos de ordenador y cualquier otro material capaz de almacenar datos e información.

La parte receptora de la información confidencial será responsable de la custodia de la misma y de cuantas copias pudiera tener, suministrada por la otra parte, en orden a su tratamiento como confidencial, secreta y restringida.

SEGUNDA. - Incumplimiento

Ambas Partes reconocen que cualquier divulgación y uso no autorizado de la Información Confidencial puede causar daños y perjuicios a la Parte Emisora que pueden resultar de difícil cuantificación. Por ello, las Partes acuerdan que la Parte Emisora tendrá derecho a reclamar ante los tribunales competentes y a obtener de la otra Parte una indemnización por los daños y perjuicios que tal divulgación y uso no autorizado le hayan generado.

TERCERA. Protección de datos

La "Parte Receptora" reconoce que la vigente legislación sobre protección de datos establece una serie de obligaciones en el tratamiento de datos de carácter personal, entre ellas, la prohibición de realizar cesiones o comunicaciones de datos sin el previo consentimiento, expreso e inequívoco de la "Parte Emisora". Asimismo, se compromete a adoptar las medidas jurídicas, técnicas y organizativas según lo establecido en el artículo 32 de RGPD.

En el supuesto de que la prestación de los servicios del presente acuerdo requiera el acceso por parte de la "Parte Receptora", a datos de carácter personal de los que es responsable la "Parte Emisora", la "Parte Receptora" cumplirá con lo dispuesto en el artículo 28 del RGPD:

- Tratará los datos personales únicamente siguiendo instrucciones documentadas de la "Parte Emisora", inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público.
- Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.
- Respetará las condiciones indicadas en los apartados 2 y 4 del artículo 28 del RGPD para recurrir a otro encargado del tratamiento.
- Asistirá a la "Parte Emisora", teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III del RGPD.
- Ayudará a la "Parte Emisora" a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36 del RGPD, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado
- A elección de la "Parte Emisora", suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

Pondrá a disposición de la "Parte Emisora" toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el artículo 28 del RGPD, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte de la "Parte Emisora" o de otro auditor autorizado por dicho responsable. El alcance de estas inspecciones o auditorías se limitará a los datos tratados por cuenta de la "Parte Emisora", será necesario preavisar a la "Parte Receptora" con una antelación mínima de 3 semanas y el coste de las mismas irá a cargo de la "Parte Emisora.

CUARTA– Duración

El presente acuerdo entra en vigor el día de su firma, y abarca cualquier información confidencial que con anterioridad ya se hubieran facilitado las partes. El acuerdo se mantendrá en vigor respecto a la información confidencial hasta que ésta deje de serlo según lo expuesto en el punto IV del Exponen, con independencia de que las relaciones comerciales entre las partes hayan terminado.

QUINTA. – Causas de resolución

El presente Acuerdo podrá resolverse, además de por cualesquiera de las causas previstas en la legislación vigente que resulten de aplicación, por las enunciadas a continuación:

a. La expiración del término contractual pactado.
b. La resolución expresa y por escrito de mutuo acuerdo.
c. El incumplimiento por una Parte de cualquiera de las obligaciones asumidas en el presente Acuerdo, siempre que tal incumplimiento no fuera subsanado en un plazo máximo de treinta (30) días naturales tras petición escrita de subsanación, a no ser que dicho incumplimiento fuese insubsanable o hiciera imposible el cumplimiento del presente Acuerdo para la Parte Informante, en cuyo caso la resolución podrá ser inmediata, y ello en todo caso dejando a salvo la reclamación que por daños y perjuicios pueda corresponder a cualquiera de las Partes.

SEXTA. - Designación de fuero.

Para la interpretación y resolución de los conflictos que pudiera surgir entre las Partes por cualquier discrepancia, cuestión o reclamación resultantes de la ejecución o interpretación del presente contrato, las Partes acuerdan intentar solucionar sus controversias a través de la mediación de un representante debidamente designado.

En todo caso, para todos los efectos derivados del presente Contrato, las partes se someten expresamente a los Juzgados y Tribunales de Barcelona, renunciando si lo hubiera a su fuero propio.

Y en prueba de su conformidad las partes firman el presente acuerdo por duplicado en el lugar y fecha abajo indicados.

“La Parte Emisora”
[entidad]

“La Parte Receptora”
[indicar]

Anexo IV.3 - MANUAL DE USO DE LA HERRAMIENTA DE CANAL DE INFORMACIÓN "OVET AUKI"

TARINAS
Law & Economy

OVET AUK

CANAL DE **COMUNICACIONES**

MANUAL DE USUARIO

CONTENIDO

- Presentación.....3
- Acceder al portal.....4
- Realizar una comunicación...6

PRESENTACIÓN

El **Canal de Comunicaciones** es un sistema a través del cual la empresa recibe y gestiona comunicaciones formuladas por sus empleados y otros miembros integrados en su organización (incluso proveedores), en relación con posibles conductas de las que hayan tenido conocimiento en un contexto laboral o profesional, y que son contrarias a las políticas, a las normas de comportamiento de algunas de las materias o entornos siguientes:

- ACOSO SEXUAL Y POR RAZÓN DE SEXO
- COMPLIANCE PENAL
- ENTORNO ESCOLAR
- ENTORNO LABORAL
- INFRACCIONES NORMATIVAS Y DE LUCHA CONTRA LA CORRUPCIÓN (LEY 2/2023, DE PROTECCIÓN A LOS INFORMANTES)
- PLAN DE IGUALDAD
- PREVENCIÓN BLANQUEO DE CAPITALES Y FT
- PREVENCIÓN RIESGOS PENALES
- OTROS

El Canal de Comunicaciones se puede adaptar a las necesidades de cada entidad.

ÁMBITO PERSONAL DE APLICACIÓN

De conformidad con la Ley 2/2023, podrán ser informantes las personas siguientes:

- TRABAJADORES POR CUENTA AJENA
- AUTÓNOMOS
- ACCIONISTAS, PARTÍCIPES Y PERSONAS PERTENECIENTES AL ÓRGANO DE ADMINISTRACIÓN, DIRECCIÓN O SUPERVISIÓN DE LA EMPRESA (CON INCLUSIÓN DE LOS MIEMBROS NO EJECUTIVOS).
- CUALQUIER PERSONA QUE TRABAJE PARA O BAJO LA SUPERVISIÓN Y LA DIRECCIÓN DE CONTRATISTAS, SUBCONTRATISTAS Y PROVEEDORES
- VOLUNTARIOS
- BECARIOS
- PERSONAL EN FORMACIÓN
- PERSONAS QUE COMUNIQUEN O REVELEN INFORMACIÓN OBTENIDA EN EL MARCO DE UNA RELACIÓN LABORAL O ESTATUTARIA YA FINALIZADA.
- PERSONAS CUYA RELACIÓN LABORAL TODAVÍA NO HA COMENZADO (ÚNICAMENTE CUANDO LA INFORMACIÓN RELATIVA A LA INFRACCIÓN SE HAYA OBTENIDO DURANTE EL PROCESO DE SELECCIÓN O NEGOCIACIÓN PRECONTRACTUAL.

ACCEDER AL PORTAL

Para acceder al **canal público** (mediante enlace web sin necesidad de registro de usuario), clicaremos en el enlace proporcionado por la Entidad y accederemos directamente al panel de alta de comunicaciones:

Clicamos en "**Realizar comunicación**" y seguimos los pasos indicados a continuación.

Para recuperar una comunicación y ver su estado hacemos clic en "**Recuperar comunicación**". Introducimos nuestro identificador único y accedemos al contenido de la misma.

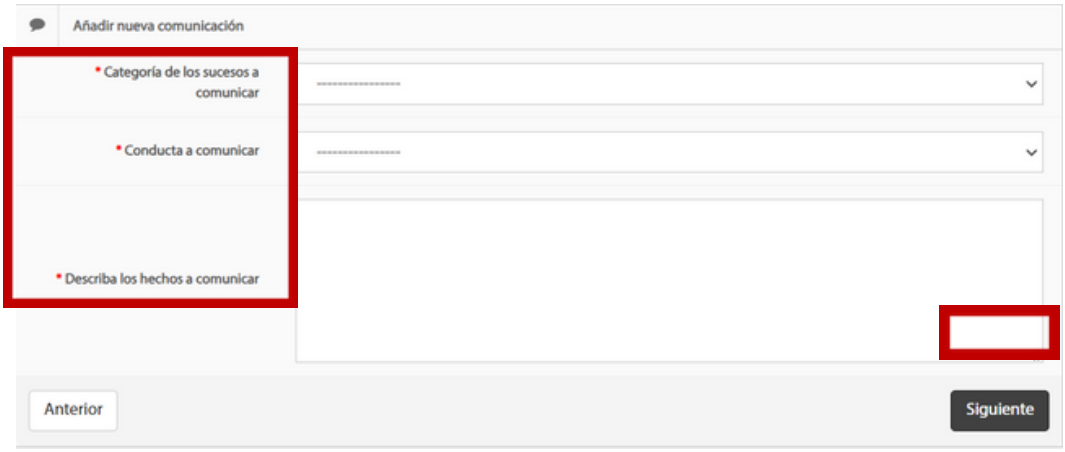
REALIZAR UNA COMUNICACIÓN

Ahora deberemos seleccionar **nuestra empresa** y aceptaremos las **condiciones** generales para continuar con el proceso de alta.

Finalmente, clicamos el botón Siguiente para pasar al próximo formulario del alta.

En el siguiente formulario introduciremos los campos básicos de **identificación** de la comunicación. Estos campos son:

- **Categoría** de los sucesos a comunicar (ámbito en el cual sucede el hecho)
- **Conducta** (subcategoría dónde especificamos el tipo de conducta comunicada)
- **Descripción** de los hechos a comunicar



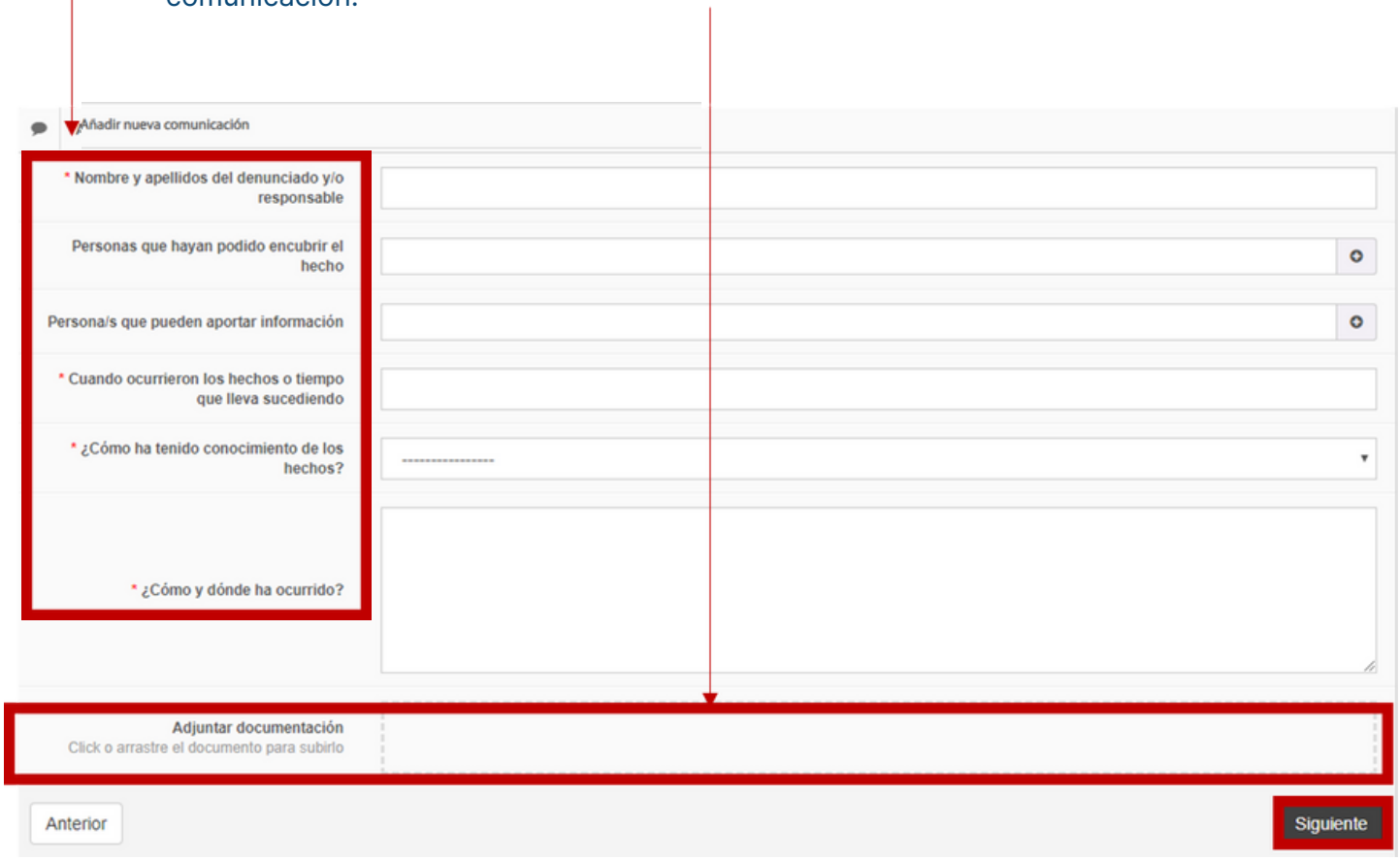
Una vez rellenados los campos indicados, clicamos el botón Siguiente para pasar al siguiente formulario del alta.

* Si el hecho que queremos comunicar no aparece en ninguna de las categorías o conductas definidas por defecto, clicaremos en “OTROS”.

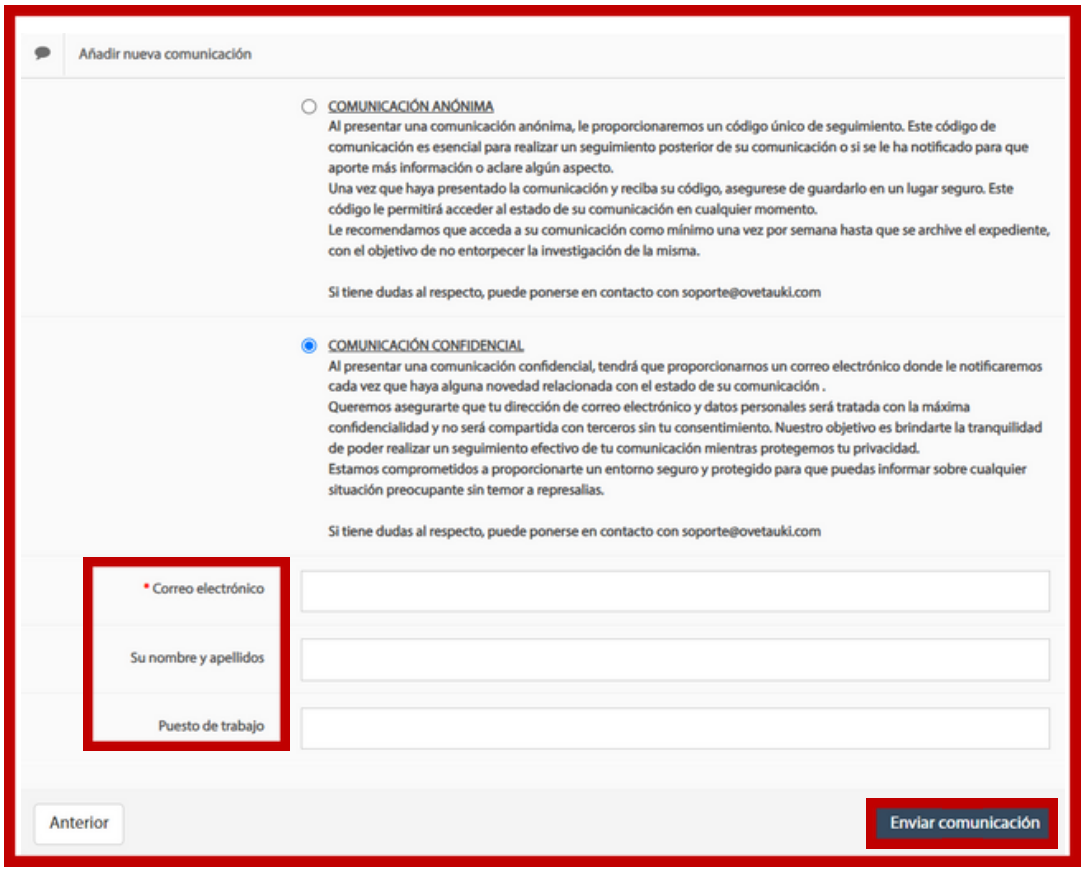
** La descripción de los hechos a comunicar ha de ser lo más rigurosa y minuciosa posible.

En el siguiente formulario introduciremos los campos que recogen **la información necesaria para gestionar la comunicación**. En este formulario constaran los datos identificativos de los sujetos denunciados, de las personas que han intervenido en los hechos o que pueden aportar información, además de especificar cuándo y dónde sucedieron dichos hechos.

También podremos adjuntar la **documentación necesaria** para complementar la comunicación.

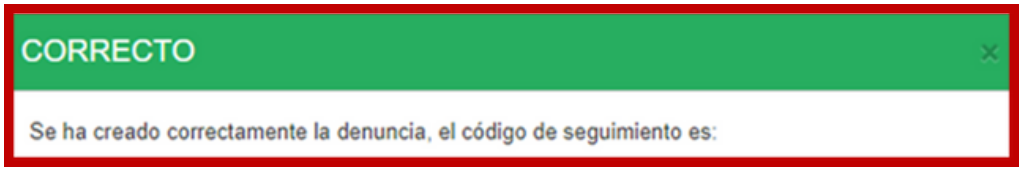


Aquí, indicaremos si deseamos crear una comunicación anónima o confidencial (leer descripción para distinguirlas) y, en caso de escoger comunicación confidencial, indicaremos nuestros datos identificativos (correo electrónico, nombre y apellidos, etc.) como sujeto que realiza la comunicación y clicaremos en "Enviar comunicación" para terminar el proceso.

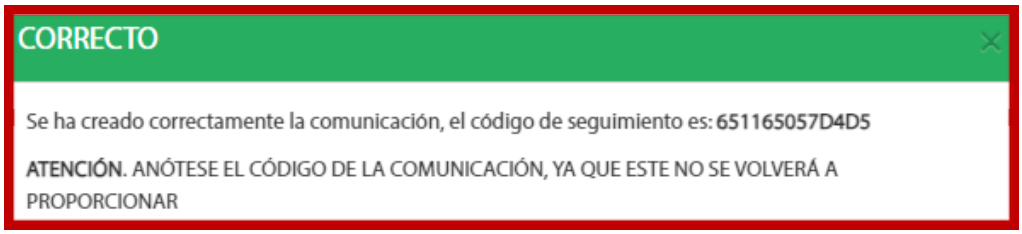


El último mensaje que nos aparecerá en pantalla nos indicará que la comunicación **se ha creado correctamente**:

Ejemplo de comunicación confidencial:



Ejemplo de comunicación anónima:



Para **consultar el estado** de una comunicación, accederemos a ella mediante el portal documental Ovet Auki (mediante el enlace proporcionado por la entidad) y presionaremos el botón **VER**.