PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES

CANAL INTERNO DE INFORMACIÓN
LEY 2/2023, DE 20 DE FEBRERO

TOGAMA, S.A.
A12075008

ESTADO DE REVISIÓN		
REVISIÓN	CONTROL DE CAMBIOS	FECHA
00	Creación del documento	22/09/2023

REALIZADO POR	REVISADO Y APROBADO POR
INGADE CONNECT S.L.	MARIANO PEREZ SANCHEZ

Contenido

1. Declaración de principios: política del sistema de gestión de informaciones

La dirección de TOGAMA, S.A. es plenamente consciente de la importancia de la colaboración ciudadana en la consecución de la plena eficacia del Derecho, yendo más allá del mero cumplimiento personal con las obligaciones que le corresponden a cada persona, sino que se extiende al compromiso colectivo con el buen funcionamiento de instituciones públicas y privadas.

La citada colaboración ciudadana se contempla además en nuestro ordenamiento jurídico como un deber de quien presencie la comisión de un delito, tal como aparece recogido en la Ley de Enjuiciamiento Criminal. En muchos casos, es gracias a esta colaboración ciudadana que, al advertir prácticas irregulares y de corrupción, han impulsado investigaciones que han concluido con la imposición de la correspondiente condena penal.

No obstante, tan importante como el deber de informar debe serlo la prohibición de represalias. En ocasiones estos loables comportamientos han generado consecuencias indeseables para quienes han comunicado tales prácticas corruptas y otras infracciones, algo que en TOGAMA, S.A. consideramos moralmente inaceptable.

Esta es la finalidad principal 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, que transpone a la Directiva 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.

Dentro de las obligaciones incluidas en esta legislación se indica que las empresas deben tener un canal interno de información. Desde TOGAMA, S.A. consideramos que siempre es preferible que la información sobre prácticas irregulares provenga de la propia organización, para así poder corregirlas o reparar lo antes posible los daños ocasionados. No hay mejor compromiso que el que una persona o entidad adquiere por propia iniciativa y convicción, como es nuestro caso.

La dirección de TOGAMA, S.A. ha implantado su canal interno de información, a través del cual todas las personas trabajadoras, personal autónomo, accionistas, partícipes y personal del órgano de administración, dirección o supervisión (incluidas personas miembro no ejecutivas) u otras personas que trabajen para o bajo la supervisión de contratistas, subcontratistas o empresas proveedoras, así como personal voluntario, becarios/as o personal en formación, podrán ejercer sus derechos de comunicación ante cualquier situación que les parezca irregular y sospechosa para que pueda ser tramitada y gestionada con la mayor celeridad.

Así mismo, desde la dirección de TOGAMA, S.A. estamos convencidos y convencidas de que la implantación efectiva de este canal interno y la transparencia y reciprocidad siempre mostrada en las comunicaciones internas nos aportarán las siguientes ventajas:

- Fomento de la transparencia y la ética empresarial, muestra del compromiso con la causa.
- Ayuda a identificar y a resolver problemas internos rápidamente
- Mejora del clima laboral interno de la empresa
- Reducción de incumplimientos legales y prevención del fraude
- Reducción de costes económicos y reputacionales
- Protección eficaz a las personas informantes frente a represalias

Se requiere de la participación y colaboración de todo el mundo, por lo que esta Política y el presente procedimiento ha sido consultado con la Representación Legal de las personas trabajadoras y es difundida a todo el personal de la empresa para su conocimiento y comprensión, así como a las partes interesadas relevantes para la organización. Para la aplicación efectiva de estos principios, es absolutamente necesario el apoyo tanto del equipo directivo como del personal.

2. Alcance

El presente Procedimiento de Gestión de Informaciones será de aplicación en aquellas circunstancias en las que dentro de la responsabilidad empresarial se vea envuelta:

- TOGAMA, S.A.
- CIF: A12075008
- DOMICILIO SOCIAL: CTRA. ONDA, KM 6. VILLARREAL, 12540 CASTELLÓN

Se debe indicar que este procedimiento afecta solamente al ámbito de esta empresa, dada su tipología como canal interno de información.

Ámbito material

Las personas físicas informantes del canal interno de información de TOGAMA, S.A. podrán aportar toda la información relevante sobre:

- Cualesquiera acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea siempre que:

    - Entren dentro del ámbito de aplicación de los actos de la Unión Europea enumerados en el anexo de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno;

    - Afecten a los intereses financieros de la Unión Europea tal y como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE);

    - 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. En todo caso, se entenderán comprendidas todas aquellas infracciones penales o administrativas graves o muy graves que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.

Ámbito personal

Podrán presentar una denuncia o aportar información mediante el canal interno de información de **TOGAMA, S.A.** sobre infracciones en un contexto laboral o profesional:

- Trabajadores y trabajadoras por cuenta ajena.
- Personal autónomo.
- Accionistas, partícipes y personas que pertenezcan al órgano de administración, dirección o supervisión de TOGAMA, S.A., incluidas personas miembro no ejecutivas.
- Cualquier persona que trabaje para o bajo la supervisión y dirección de empresas contratistas, subcontratistas y proveedoras.

Además de las anteriores podrán comunicar o revelar información sobre infracciones obtenida en el marco de una relación laboral ya finalizada, personal voluntario, becarios y becarias, personal en periodo de formación (con o sin remuneración) y personal cuya relación laboral no haya empezado todavía pero que hayan obtenido la información sobre infracciones durante el proceso de selección o de negociación precontractual.

Las medidas de protección que se detallarán en posteriores apartados serán también de aplicación, en su caso, a:

- Personas físicas que, en el marco de la organización en la que preste servicios la persona informante, asistan a la misma en el proceso,
- Personas físicas que estén relacionadas con la persona informante y que puedan sufrir represalias, como compañeros y compañeras de trabajo o familiares de la persona informante
- 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. Periodo de vigencia

El presente Procedimiento tendrá una vigencia de **UN AÑO** desde la fecha de su aprobación, considerándose tácitamente renovado por períodos iguales si no hay solicitud expresa ni por parte de la empresa ni por parte de la representación legal de las personas trabajadoras.

Se actualizará periódicamente a medida que vayan existiendo cambios legislativos que así lo requieran.

4. Definiciones

- Agencia Española de Protección de datos: según la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, es la autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones. Corresponde a la Agencia Española de Protección de Datos:

    - Supervisar la aplicación de esta ley orgánica y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo reglamento, en la presente ley orgánica y en sus disposiciones de desarrollo.

    - Desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea.

- Autoridad de control: según el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016, se define autoridad de control la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto al artículo 51 de este reglamento. En el caso de España, se trataría de la Agencia Española de Protección de Datos.

- Autoridad Independiente del Informante (AII): es la autoridad independiente, creada en base a los requisitos de la Ley 2/2023, de 20 de febrero, con competencias para la tramitación, a través del canal externo, de las informaciones que afecten a los siguientes sujetos (salvo creación y atribución de competencias a autoridades autonómicas que actúen en su nombre):

    - La Administración General del Estado y entidades que integran el sector público estatal.

    - Resto de entidades del sector público, los órganos constitucionales y los órganos de relevancia constitucional a que se refiere el artículo 13.

    - Entidades que integran el sector privado, cuando la infracción o el incumplimiento sobre el que se informe afecte o produzca sus efectos en el ámbito territorial de más de una comunidad autónoma.

    - Cuando se suscriba el oportuno convenio, las Administraciones de las comunidades autónomas, las entidades que integran la Administración y el sector público institucional autonómico o local.

- Canal interno de información: herramienta para posibilitar la presentación de información respecto de las infracciones previstas en el artículo 2 de la ley 2/2023, de 20 de febrero, estará integrado dentro del Sistema interno de información a que se refiere el artículo 5 de la misma ley. Se trata de un instrumento que deberá permitir realizar comunicaciones por escrito o verbalmente, o de las dos formas. La información se podrá realizar bien por escrito, a través de correo postal o a través de cualquier medio electrónico habilitado al efecto, o verbalmente, por vía telefónica o a través de sistema de mensajería de voz. A solicitud del informante, también podrá presentarse mediante una reunión presencial dentro del plazo máximo de siete días. Obligatorio que dispongan de él:

- En el sector privado:
  - Las personas físicas o jurídicas del sector privado que tengan contratados cincuenta o más personas trabajadoras.
  - 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 personas trabajadoras con que cuenten. En estos casos, esta ley será de aplicación en lo no regulado por su normativa específica.
  - Los partidos políticos, los sindicatos, las organizaciones empresariales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos
- En el sector público: todas las entidades que integran el sector público:
  - La Administración General del Estado, las Administraciones de las comunidades autónomas, ciudades con Estatuto de Autonomía y las entidades que integran la Administración Local.
  - Los organismos y entidades públicas vinculadas o dependientes de alguna Administración pública, así como aquellas otras asociaciones y corporaciones en las que participen las Administraciones y organismos públicos.
  - Las autoridades administrativas independientes, el Banco de España y las entidades gestoras y servicios comunes de la Seguridad Social.
  - Las universidades públicas.
  - Las corporaciones de Derecho público.
  - Las fundaciones del sector público. A efectos de esta ley, se entenderá por fundaciones del sector público aquellas que reúnan alguno de los siguientes requisitos:
    - 1.º Que se constituyan de forma inicial, con una aportación mayoritaria, directa o indirecta, de una o varias entidades integradas en el sector público, o bien reciban dicha aportación con posterioridad a su constitución.
    - 2.º Que el patrimonio de la fundación esté integrado en más de un cincuenta por ciento por bienes o derechos aportados o cedidos por sujetos integrantes del sector público con carácter permanente.

- 3.º Que la mayoría de derechos de voto en su patronato corresponda a representantes del sector público.

- g) Las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de entidades de las mencionadas en las letras a), b), c), d) y g) del presente apartado sea superior al cincuenta por ciento, o en los casos en que, sin superar ese porcentaje, se encuentre respecto de las referidas entidades en el supuesto previsto en el artículo 5 del texto refundido de la Ley del Mercado de Valores, aprobado por Real Decreto Legislativo 4/2015, de 23 de octubre.

- Dato de carácter personal: según el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016, se definen los datos personales como toda información sobre una persona física identificada o identificable («el interesado»);
  - Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

- Delegado/a de protección de datos: según la ley orgánica 3/2018, de 5 de diciembre, El delegado o delegada de protección de datos actuará como interlocutor/a del responsable o encargado/a del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado o delegada podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias. Los y las responsables y encargados/as del tratamiento deberán designar un delegado/a de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

  - Los colegios profesionales y sus consejos generales.

  - Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

  - Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

  - Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

  - Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

  - Los establecimientos financieros de crédito.

  - Las entidades aseguradoras y reaseguradoras.

- Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
- Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
- Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.
- Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.
- Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.
- Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.
- Las empresas de seguridad privada.
- Las federaciones deportivas cuando traten datos de menores de edad.

- **Encargado/a de tratamiento**: definido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 como la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable de tratamiento. En este caso sería el gestor o la gestora del canal interno de información / denuncias.

- **HTTPS** (protocolo de transferencia de hipertexto seguro): es una versión encriptada de HTTP, que es el protocolo más usado para transferir datos en internet. HTTPS protege la comunicación entre navegador y servidor para que no sea interceptada o modificada por atacantes. El HTTPS está encriptado para aumentar la seguridad de las transferencias de datos. Esto es especialmente importante cuando los usuarios y usuarias transmiten datos confidenciales. En los navegadores modernos, como Chrome, los sitios web que no utilizan HTTPS se señalan de forma diferente a los que sí lo hacen. Identifica un candado en la barra de URL que indicará que la página web es segura. HTTPS utiliza un protocolo de encriptación (TLS, antes SSL) para encriptar las comunicaciones. Este protocolo asegura las comunicaciones mediante el uso de lo que se conoce como infraestructura de clave pública asimétrica. Este tipo de sistema de seguridad utiliza dos claves diferentes para encriptar las comunicaciones entre dos partes:

- La clave privada: esta clave la controla el propietario/a de un sitio web y se mantiene privada. Esta clave está ubicada en un servidor web y se utiliza para desencriptar la información encriptada por la clave pública.

- La clave pública: esta clave está disponible para quienes quieran interactuar con el servidor de forma segura. La información encriptada por la clave pública sólo puede ser desencriptada por la clave privada.

- **Informante/a** (denunciante/a o alertador/a o *whistleblower*): persona que transmite una determinada información. En este contexto está relacionada con infracciones (acciones u omisiones) constitutivas de infracción penal o administrativa grave a través de los canales externos o internos de información.

- **Infracción administrativa**: Acción u omisión típica, antijurídica y culpable para la que el ordenamiento jurídico prevé la imposición de una sanción administrativa, no privativa de libertad. Sus elementos esenciales coinciden con los del delito.

- **Infracción penal**: Son delitos o faltas las acciones y omisiones dolosas o imprudentes penadas por la Ley; formalmente son infracciones penales las acciones u omisiones que infringen una ley penal, y, materialmente son infracciones penales las tipificadas en la ley penal. Para que la conducta sea considerada infracción penal deben cumplirse los siguientes requisitos:

  - Tipicidad: la conducta infractora está recogida en una ley penal
  - Antijuridicidad: la constatación de que el hecho producido es contrario a derecho, injusto o ilícito.
  - Culpabilidad: Para que exista culpabilidad es necesario que el sujeto tenga conciencia y conocimiento de la antijuricidad del hecho, es decir, que sea imputable
  - Además de lo anterior, hay que tener en cuenta la punibilidad.

- **IP** (Protocolo de Internet): una dirección IP es una etiqueta numérica que identifica de manera lógica y jerárquica una interfaz (habitualmente un dispositivo) conectada a una red, que utilice el protocolo de internet o que corresponda al nivel de red del modelo TCP/IP. Una dirección IP tiene dos funciones principales: identificación de la interfaz de red y direccionamiento para su ubicación. La dirección IP puede cambiar a menudo debido a cambios en la red, o porque el dispositivo encargado dentro de la red de asignar las direcciones IP, decida asignar otra IP. Los dispositivos se conectan entre sí mediante sus respectivas direcciones IP.

- **Limitación de tratamiento**: definido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 como el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

- **Metadatos**: aquellos datos que hablan de los datos, es decir, describen el contenido de los archivos o la información de los mismos. Importante tenerlos bajo control en el canal de información para mantener privada la información personal. Se caracterizan por:

  - Ser datos altamente estructurados que describen características de los datos, como el contenido, calidad, información y otras circunstancias o atributos.

- Presentan diferenciaciones que dependen, en última instancia, de las reglas incluidas en las aplicaciones para determinar la estructura interna de los esquemas de datos.
- Pueden clasificarse en función de distintos criterios, como su contenido, variabilidad o función

- MFA (autenticación multifactor): Es un método de control de acceso informático en el que a un usuario o usuaria se le concede acceso al sistema solo después de que presente dos o más pruebas diferentes de que es quien dice ser. Los factores de autenticación de un patrón de autenticación de múltiples factores podrían incluir:

  - Algún objeto físico en posesión del usuario o usuaria, como una memoria USB con un identificador único, una tarjeta de crédito, una llave, etc.

  - Algún secreto conocido por el usuario o usuaria, como una contraseña, un pin, …

  - Alguna característica biométrica propia del usuario o usuaria, como una huella dactilar, iris, voz, velocidad de escritura, patrón en los intervalos de pulsación de teclas, entre otros.

- Prácticas corruptas: son todo tipo de actos deshonestos o delictivos. Las formas de corrupción varían, pero las más comunes son el uso ilegítimo de información privilegiada y el patrocinio; además de los sobornos, el tráfico de influencias, la evasión fiscal, las extorsiones, los fraudes, la malversación, la prevaricación, el caciquismo, el compadrazgo, la cooptación, el nepotismo, la impunidad y el despotismo.

- Procedimiento de gestión de información: definido en la ley 2/2023, de 20 de febrero como procedimiento que establece las previsiones necesarias para que el Sistema interno de información y los canales internos de información existentes cumplan con los requisitos establecidos en esta ley. En particular, el procedimiento responderá al contenido mínimo y principios siguientes:

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

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

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

  - Determinación del plazo máximo para dar respuesta a las actuaciones de investigación, que no podrá ser superior a tres meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo a la persona informante, a tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, éste podrá extenderse hasta un máximo de otros tres meses adicionales.

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

- Establecimiento del derecho de la persona afectada a que se le informe de las acciones u omisiones que se le atribuyen, y a ser oída en cualquier momento. Dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.

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

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

- Respeto de las disposiciones sobre protección de datos personales de acuerdo a lo previsto en el título VI.

- Remisión de la información al Ministerio Fiscal con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

- Responsable del sistema interno de información: según la Ley 2/2023, de 20 de febrero, el órgano de administración u órgano de gobierno de cada entidad u organismo obligado por esta ley será el competente para la designación de la persona física responsable de la gestión de dicho sistema o «Responsable del Sistema», y de su destitución o cese.

    - Tanto el nombramiento como el cese de la persona física individualmente designada, así como de las integrantes del órgano colegiado deberán ser notificados a la Autoridad Independiente de Protección del Informante, A.A.I., o, en su caso, a las autoridades u órganos competentes de las comunidades autónomas, en el ámbito de sus respectivas competencias, en el plazo de los diez días hábiles siguientes, especificando, en el caso de su cese, las razones que han justificado el mismo.

    - El responsable del Sistema deberá desarrollar sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad u organismo, no podrá recibir instrucciones de ningún tipo en su ejercicio, y deberá disponer de todos los medios personales y materiales necesarios para llevarlas a cabo.

    - En el caso del sector privado, el responsable del Sistema persona física o la entidad en quien el órgano colegiado responsable haya delegado sus funciones, será un *directivo de la entidad*, que ejercerá su cargo con independencia del órgano de administración o de gobierno de la misma. Cuando la naturaleza o la dimensión de las actividades de la entidad no justifiquen o permitan la existencia de un directivo Responsable del Sistema, será posible el desempeño ordinario de las funciones del puesto o cargo con las de responsable del Sistema, tratando en todo caso de evitar posibles situaciones de conflicto de interés.

    - En las entidades u organismos en que ya existiera una *persona responsable de la función de cumplimiento normativo o de políticas de integridad*, cualquiera que fuese su denominación,

podrá ser esta la persona designada como responsable del Sistema, siempre que cumpla los requisitos establecidos en esta ley.

- **Responsable de tratamiento**: definido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 como persona física o jurídica, autoridad pública, servicio u otros organismos que, solo/a o junto con otros/as, determine los fines y medios de tratamiento. En este contexto, el órgano de administración u órgano de gobierno de cada entidad u organismo obligado por la ley 2/2023, de 20 de febrero, será el responsable de la implantación del Sistema interno de información, previa consulta con la representación legal de las personas trabajadoras, y tendrá la condición de responsable del tratamiento de los datos personales de conformidad con lo dispuesto en la normativa sobre protección de datos personales

- **Sistema interno de información**: Según ley 2/2023, de 20 de febrero, deberá:

  - Permitir a todas las personas referidas en el artículo 3 comunicar información sobre las infracciones previstas en el artículo 2.

  - Estar diseñado, establecido y gestionado de una forma segura, de modo que se garantice la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la protección de datos, impidiendo el acceso de personal no autorizado.

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

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

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

  - Ser independientes y aparecer diferenciados respecto de los sistemas internos de información de otras entidades u organismos, sin perjuicio de lo establecido en los artículos 12 y 14.

  - Contar con una persona responsable del sistema.

  - Contar con una política o estrategia que enuncie los principios generales en materia de Sistemas interno de información y defensa del informante y que sea debidamente publicitada en el seno de la entidad u organismo.

  - Contar con un procedimiento de gestión de las informaciones recibidas.

  - Establecer las garantías para la protección de los y las informantes en el ámbito de la propia entidad u organismo, respetando, en todo caso, lo dispuesto en el artículo 9.

- **SHA** (algoritmos de hash seguro): familia de funciones de hash criptográficas publicadas por el Instituto Nacional de Estándares y Tecnología (NIST) como un estándar federal de procesamiento de información (FIPS) de EE. UU.

- Una característica principal de las funciones SHA es la capacidad de no reflexividad, es decir, dado una cadena de bits del buffer de salida resulta prácticamente imposible intentar hallar una cadena origen que devuelva el mismo contenido, además de disponer de una gran cantidad de combinaciones posibles que evitan que se puedan dar duplicado de datos o colisiones las cuales pueden comprometer la seguridad de diferentes archivos.

- Las funciones SHA permiten la creación de cadenas diferentes que facilitan seguir un registro de cambios en la seguridad de diferentes archivos conocida como huella digital, esto sirve de especial importancia en aplicaciones tales como la creación de cuentas asociadas a contraseñas que solo un usuario debe conocer, claves de encriptado de ficheros o usos en la creación de cadenas de bloques en criptomonedas como el bitcoin.

- SSL (*Secure Sockets Layer*): protocolo de navegadores y servidores web que permite autenticar, cifrar y descifrar la información enviada a través de internet, haciendo que sea seguro transmitir información confidencial, como datos personales, de pagos o de inicio de sesión. Puedes saber si un sitio web está usando un certificado porque verás un pequeño ícono de candado junto a la URL en la barra de direcciones.

- TLS (*Transport Layer Security*): es un protocolo de seguridad ampliamente adoptado, diseñado para facilitar la privacidad y la seguridad de los datos en las comunicaciones por Internet. Un caso de uso primario de TLS es la encriptación de las comunicaciones entre aplicaciones web y servidores, como los navegadores que cargan un sitio web. TLS también puede usarse para encriptar otras comunicaciones como el correo electrónico, los mensajes y la voz sobre IP (VoIP). TLS surge a partir de un protocolo de encriptación SSL.

- Tratamiento de datos personales: definido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

- *Whistleblowing* (denuncia de irregularidades): se produce cuando una persona informa de una infracción en una organización, por ejemplo, de una mala conducta financiera o de un caso de discriminación. Esta persona suele ser una persona trabajadora, pero también puede ser un tercero/a, como una empresa proveedora o un cliente o clienta.

    - El objetivo principal de la normativa es asegurar que cualquier persona trabajadora tenga a su disposición un instrumento que le facilite la revelación de posibles infracciones o irregularidades que puedan estar ocurriendo en la empresa.
    - La Directiva *Whistleblowing* deja, además, claramente establecida la necesidad de garantizar la confidencialidad de la persona denunciante o alertador/a. En resumen, se busca promover un entorno más ético en la empresa habilitando opciones de denuncia de conductas ilícitas y, garantizando a su vez, la protección de la persona denunciante (*whistleblower*, en inglés).

5. Procedimiento de gestión de informaciones

Para gestionar adecuadamente la información aportada por las personas informantes se crea el presente procedimiento de gestión de información. El procedimiento establecerá las previsiones necesarias para que el Sistema interno de información y los canales internos de información existentes cumplan con los requisitos establecidos en la ley 2/2023, de 20 de febrero. En particular, el procedimiento responderá al contenido mínimo y principios siguientes:

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

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

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

d) Determinación del **plazo máximo para dar respuesta** a las actuaciones de investigación, que no podrá ser superior a tres meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo a la persona informante, a tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, éste podrá extenderse hasta un máximo de otros tres meses adicionales.

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

f) Establecimiento del **derecho de la persona afectada a que se le informe de las acciones u omisiones que se le atribuyen**, y a ser oída en cualquier momento. Dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.

g) **Garantía de la confidencialidad** cuando la comunicación sea remitida por canales de denuncia que no sean los establecidos o a miembros del personal no responsable de su tratamiento, al que se habrá formado en esta materia y advertido de la tipificación como infracción muy grave de su quebranto y,

asimismo, el establecimiento de la obligación del receptor de la comunicación de remitir inmediatamente a la persona Responsable del Sistema.

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

i) Respeto de las **disposiciones sobre protección de datos personales** de acuerdo a lo previsto en el título VI 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.

j) **Remisión de la información al Ministerio Fiscal** con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la **Fiscalía Europea**.

A continuación, en los posteriores apartados se darán indicaciones precisas sobre la forma de proceder para aportar información a los canales establecidos y cómo será su funcionamiento y tramitación de expedientes.

5.1 Funcionamiento del canal de denuncias interno

El canal interno de información para tramitar las denuncias e informaciones relacionadas con acciones u omisiones constitutivas de infracción administrativa grave o muy grave o penal se realizarán a través del canal habilitado por **TOGAMA, S.A.**, al que se puede acceder en el siguiente enlace: https://ingade-reporting.com/togama-sa-home/.

Este enlace se encuentra habilitado y redireccionado desde la web de la empresa en su página de inicio, en una sección separada y fácilmente identificable, como dicta la Ley 2/2023, de 20 de febrero.

En el caso de **TOGAMA, S.A.**, la información se encuentra en https://togama.com/, al pie de la página de inicio. En la parte izquierda, sobre los enlaces de aviso legal y políticas de privacidad y cookies, se encuentra el enlace identificado como "Canal de denuncias" sobre fondo azul.

Las denuncias realizadas serán tramitadas por la persona responsable del sistema mediante recepción de las informaciones recibidas y su posterior investigación tal como se describe en posteriores apartados, siendo el

órgano de gestión de la empresa el Responsable del Tratamiento de Datos Personales y la persona responsable del sistema y la empresa de consultoría encargados del tratamiento de datos.

Nombramiento de la persona Responsable del sistema interno de información

El órgano de administración u órgano de gobierno de **TOGAMA, S.A.** será el ente competente para la designación de la persona física responsable de la gestión de dicho sistema o «Responsable del Sistema», y de su destitución o cese.

Si se optase por que el Responsable del Sistema fuese un órgano colegiado, éste deberá delegar en una de sus personas miembro las facultades de gestión del Sistema interno de información y de tramitación de expedientes de investigación.

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

El Responsable del Sistema deberá desarrollar sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad u organismo, no podrá recibir instrucciones de ningún tipo en su ejercicio, y deberá disponer de todos los medios personales y materiales necesarios para llevarlas a cabo.

En el caso del sector privado, y más concretamente de **TOGAMA, S.A.,** la persona Responsable del Sistema persona física o la entidad en quien el órgano colegiado responsable haya delegado sus funciones, será personal directivo de la entidad, que ejercerá su cargo con independencia del órgano de administración o de gobierno de la misma. Cuando la naturaleza o la dimensión de las actividades de la entidad no justifique o permita la existencia de personal directivo Responsable del Sistema, será posible el desempeño ordinario de

las funciones del puesto o cargo con las de Responsable del Sistema, tratando en todo caso de evitar posibles situaciones de conflicto de interés.

En caso de que en **TOGAMA, S.A.** existiese una persona responsable de la función de cumplimiento normativo o de políticas de integridad, cualquiera que fuese su denominación, podrá ser esta la persona designada como Responsable del Sistema, siempre que cumpla los requisitos establecidos en esta ley.

En los anexos del presente procedimiento se dispone de un modelo de aceptación del cargo de responsable y de comunicación a la A.A.I., que puede ser usado para tal fin al llevarse a cabo un nombramiento nuevo.

5.1.1 Recepción de la información

Información aportada por la persona denunciante: denuncia anónima o con identidad reservada

El primer paso para aportar información implica acceder al enlace del canal interno de denuncias de **TOGAMA, S.A.**. Las informaciones aportadas pueden llevarse a cabo **de forma anónima** o **con identidad reservada**, según las directrices del artículo 33 de la Ley 2/2023, de 20 de febrero, debiendo adoptarse las medidas pertinentes.

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

La identidad de la persona informante solamente podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora. Las revelaciones hechas estarán sujetas a salvaguardas establecidas en la normativa aplicable. En particular, se trasladará a la persona informante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial. Cuando la autoridad competente lo comunique a la persona informante, le remitirá un escrito explicando los motivos de la revelación de los datos confidenciales en cuestión.

- Para realizar la denuncia de forma anónima puede escoger no facilitar su nombre, apellidos, dirección de email ni teléfono en los campos habilitados para tal fin, añadiendo únicamente el campo de "descripción". Es importante que incluya toda la información y evidencias posibles, ya que al no facilitar datos de contacto no será posible que la persona encargada de tramitar no va a poder requerir información adicional durante la investigación.

- Para realizar la denuncia sin ser anónima, incluyendo sus datos personales y de contacto, aparte de la descripción. Sus datos personales serán debidamente tratados y asignados a un código localizador que será el que se utilice en las comunicaciones entre usted y la persona que tramite la investigación.

Al presentar la información, la persona informante podrá indicar un **domicilio**, **correo electrónico** o **lugar seguro** a efectos de recibir las notificaciones, pudiendo asimismo renunciar expresamente a la recepción de cualquier comunicación de actuaciones llevadas a cabo como consecuencia de la información aportada.

Formas de presentación de informaciones y denuncias

La información se podrá realizar de tres posibles formas:

- Por escrito: a través de correo postal o electronicamente mediante el formulario web anteriormente explicado o a través del email de denuncias@ingade.es. Si la comunicación se realiza por correo postal se deberá enviar a la siguiente dirección: **Parque Tecnolóxico de Galicia, Tecnópole I, local 13 – CP 32900 San Cibrao das Viñas (Ourense).**

- Verbal: por vía telefónica llamando al teléfono habilitado para tal fin: 988 808 664 o enviando el audio/vídeo mediante el formulario web.

- En reunión presencial: si la persona informante así lo decide, puede presentar su denuncia mediante una reunión presencial o por videollamada. Si se realiza por esta vía, el plazo máximo entre la solicitud de reunión y la reunión efectiva no podrá exceder el plazo de 7 días.

Siempre que la información se facilite verbalmente (incluida reunión presencial), se advierte a la persona informante que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo con lo que establecen el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre. Además, se documentará la llamada, audio/vídeo o reunión presencial dejando evidencia documentada de la misma:

- Mediante grabación de la conversación en un formato seguro, duradero y accesible. En este supuesto se valorará la necesidad de pasar la grabación por un distorsionador de voz para proteger la identidad de la persona informante.

- A través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla. Sin perjuicio de los derechos que le corresponden de acuerdo a la normativa sobre protección de datos, se ofrecerá a la persona informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción del mensaje.

Presentada la información, se procederá a su registro en el Sistema de Gestión de Información de **TOGAMA, S.A.**, siéndole asignado un código de identificación para mantener la trazabilidad durante todo el proceso. El Sistema de Gestión de Información estará contenido en una base de datos segura y de acceso restringido exclusivamente al personal convenientemente autorizado, en la que se registrarán todas las comunicaciones recibidas, cumplimentando los siguientes datos:

a) Fecha de recepción.

b) Código de identificación.

c) Actuaciones desarrolladas.

d) Medidas adoptadas.

e) Fecha de cierre.

Acuse de recibo

Recibida la información, en un plazo no superior a **cinco días hábiles** desde dicha recepción se procederá a acusar recibo de la misma, a menos que la persona informante expresamente haya renunciado a recibir comunicaciones relativas a la investigación o que la persona Responsable del sistema interno de información considere razonablemente que el acuse de recibo de la información comprometería la protección de la identidad de la persona informante.

5.1.2 Admisión y supuestos de inadmisión

Una vez que la información haya sido registrada en el canal interno de información de **TOGAMA, S.A.**, la persona responsable del sistema interno de información deberá comprobar si aquella expone hechos o conductas que se encuentran dentro del ámbito de aplicación, que se indica a continuación:

- Cualesquiera **acciones u omisiones** que puedan constituir infracciones del Derecho de la Unión Europea siempre que:
    - Entren dentro del ámbito de aplicación de los actos de la Unión Europea enumerados en el anexo de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno;
    - Afecten a los intereses financieros de la Unión Europea tal y como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE); o
    - Incidan en el mercado interior, tal y como se contempla en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión Europea en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades o con prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades.
- **Acciones u omisiones** que puedan ser constitutivas de infracción penal o administrativa grave o muy grave. En todo caso, se entenderán comprendidas todas aquellas infracciones penales o

administrativas graves o muy graves que impliquen quebranto económico para la *Hacienda Pública* y para la *Seguridad Social*.

Supuestos de inadmisión y plazos

Una vez la persona responsable del sistema interno de información ha realizado el análisis preliminar anteriormente descrito, decidirá, en un plazo que no podrá ser superior a **cinco días hábiles** desde la fecha de entrada en el registro de la información:

- Inadmitir la comunicación, en alguno de los siguientes casos:
    - Cuando los hechos relatados carezcan de toda verosimilitud.
    - Cuando los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico incluida en el ámbito de aplicación de esta ley.
    - Cuando la comunicación carezca manifiestamente de fundamento o existan, a juicio de la persona responsable del sistema interno de información, indicios racionales de haberse obtenido mediante la comisión de un delito. En este último caso, además de la inadmisión, se remitirá al Ministerio Fiscal relación circunstanciada de los hechos que se estimen constitutivos de delito.
    - Cuando la comunicación no contenga información nueva y significativa sobre infracciones en comparación con una comunicación anterior respecto de la cual han concluido los correspondientes procedimientos, a menos que se den nuevas circunstancias de hecho o de Derecho que justifiquen un seguimiento distinto. En estos casos, la persona responsable del sistema interno de información notificará la resolución de manera motivada.

La inadmisión se comunicará a la persona informante dentro de los **cinco días hábiles siguientes**, salvo que la comunicación fuera anónima o la persona informante hubiera renunciado a recibir comunicaciones de la persona responsable del sistema interno de información.

- Remitir con carácter inmediato la información al Ministerio Fiscal cuando los hechos pudieran ser **indiciariamente constitutivos de delito** o a la Fiscalía Europea en el caso de que los **hechos afecten a los intereses financieros de la Unión Europea**.

- Remitir la comunicación a la autoridad, entidad u organismo que se considere competente para su tramitación. En caso de que lleguen por esta vía informaciones fuera del ámbito de aplicación de la ley 2/2023, de 20 de febrero, se remitirá a la autoridad competente para su tramitación. Se aplica a:
    - Personas informantes que trabajan en el sector privado o público y que hayan obtenido información sobre infracciones en un contexto laboral o profesional, comprendiendo en todo caso:
        - Las personas que tengan la condición de trabajadores o trabajadoras por cuenta ajena;

- Los autónomos y las autónomas;
- Los y las accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de TOGAMA, S.A., incluidos los miembros no ejecutivos;
- Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

- También se aplicará a los y las informantes que comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral o estatutaria ya finalizada, voluntarios/as, becarios y becarias, personas trabajadoras en periodos de formación con independencia de que perciban o no una remuneración, así como a aquellas 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.

En cualquier otro supuesto, la información pasará a fase de admisión a trámite.

Admisión a trámite y notificación a la persona informante

La admisión a trámite se comunicará a la persona informante dentro de los **cinco días hábiles** siguientes, salvo que la comunicación fuera anónima o la persona informante hubiera renunciado a recibir comunicaciones de la persona responsable del sistema interno de información.

5.1.3 Instrucción

Una vez que la información ha sido recibida y admitida a trámite comienza la fase de instrucción, en la que se incluyen todos los pasos para verificar la verosimilitud de los hechos relatados.

Se garantizará que la persona afectada por la información tenga noticia de la misma, así como de los hechos relatados de manera sucinta. Adicionalmente se le informará del derecho que tiene a presentar alegaciones por escrito y del tratamiento de sus datos personales. No obstante, esta información podrá efectuarse en el **trámite de audiencia** si se considerara que su aportación con anterioridad pudiera facilitar la ocultación, destrucción o alteración de las pruebas.

En ningún caso se comunicará a los sujetos/as afectados/as la identidad de la persona informante ni se dará acceso a la comunicación. Durante la instrucción se dará noticia de la comunicación con sucinta relación de hechos a la persona investigada. Esta información podrá efectuarse en el **trámite de audiencia** si se considera que su aportación con anterioridad pudiera facilitar la ocultación, destrucción o alteración de las pruebas.

Sin perjuicio del derecho a formular alegaciones por escrito, la instrucción comprenderá, siempre que sea posible, una **entrevista con la persona afectada** en la que, siempre con absoluto respeto a la presunción de inocencia, se le invita a exponer su versión de los hechos y a aportar aquellos medios de prueba que considere adecuados y pertinentes.

A fin de garantizar el derecho de defensa de la persona afectada, la misma tendrá acceso al expediente sin revelar información que pudiera identificar a la persona informante, pudiendo ser oída en cualquier momento, y se le advertirá de la posibilidad de comparecer asistida de abogado.

La persona responsable del sistema interno de información y otras personas autorizadas que desarrollen actividades de investigación estarán obligados y obligadas a guardar secreto sobre las informaciones que conozcan con ocasión de dicho ejercicio.

Todas las personas naturales o jurídicas, privadas o públicas, deberán colaborar con las autoridades competentes y estarán obligadas a atender los requerimientos que se les dirijan para aportar documentación,

datos o cualquier información relacionada con los procedimientos que se estén tramitando, incluso los datos personales que le fueran requeridos.

5.1.4 Terminación de actuaciones y toma de decisiones

Una vez finalizada la fase de instrucción y tras haber recabado todas las pruebas o informaciones pertinentes de las partes interesadas, la persona responsable del sistema interno de información emitirá un informe, que contenga, al menos:

- Una exposición de los hechos relatados junto con el código de identificación de la comunicación y la fecha de registro.
- El tipo de comunicación recibida y su tipología a efectos de conocer su prioridad o no en su tramitación y el cauce que va a seguir para su tramitación.
- Las actuaciones realizadas con el fin de comprobar la verosimilitud de los hechos.
- Las conclusiones alcanzadas en la instrucción y la valoración de las diligencias y de los indicios que las sustentan.

Una vez emitido el informe al menos con esos contenidos mínimos, la persona responsable del sistema interno de información adoptará alguna de las decisiones que se enlistan a continuación:

- Archivo del expediente, que será notificado a la persona informante y, en su caso, a la persona afectada. En estos supuestos, la persona informante tendrá **derecho a la protección** prevista en la ley 2/2023, de 20 de febrero, salvo que, como consecuencia de las actuaciones llevadas a cabo en fase de instrucción, se concluya que la información a la vista de la información recabada, debía haber sido inadmitida por concurrir alguna de las causas previstas.
- Remisión al Ministerio Fiscal si, pese a no apreciar inicialmente indicios de que los hechos pudieran revestir el carácter de delito, así resultase del curso de la instrucción. Si el delito afectase a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.
- Traslado de todo lo actuado a la autoridad competente para su tramitación en caso de que exceda las competencias de **TOGAMA, S.A.**
- Adopción de acuerdo de inicio de un procedimiento sancionador en los términos previstos en el título IX de la Ley 2/2023, de 20 de febrero.

El plazo para finalizar las actuaciones y dar respuesta a la persona informante, en su caso, no podrá ser superior a **tres meses desde la entrada en registro de la información**. Cualquiera que sea la decisión, se comunicará a la persona informante, salvo que haya renunciado a ello o que la comunicación sea anónima.

La presentación de una comunicación por la persona informante no le confiere, por sí sola, la condición de persona interesada.

5.1.5 Garantías del procedimiento

Las personas informantes contarán con las siguientes garantías en dentro del Procedimiento de gestión de informaciones y ante la persona responsable del sistema interno de información:

- Decidir si desea formular la comunicación de forma anónima o no anónima; en este segundo caso se garantizará la reserva de identidad de la persona informante, de modo que esta no sea revelada a terceras personas mediante un código identificador único.

- Formular la comunicación verbalmente o por escrito, o en reunión presencial o por videollamada a petición de la persona informante.

- Indicar un domicilio, correo electrónico o lugar seguro donde recibir las comunicaciones que realice la Autoridad Independiente de Protección del Informante, A.A.I. a propósito de la investigación.

- Renunciar, en su caso, a recibir comunicaciones de la persona responsable del sistema interno de información.

- Comparecer ante la persona responsable del sistema interno de información, por propia iniciativa o cuando sea requerido por esta, siendo asistida, en su caso y si lo considera oportuno, por un abogado o abogada.

- Solicitar a la persona responsable del sistema interno de información que la comparecencia ante la misma sea realizada por videoconferencia u otros medios telemáticos seguros que garanticen la identidad de la persona informante, y la seguridad y fidelidad de la comunicación.

- Ejercer los derechos que le confiere la legislación de protección de datos de carácter personal.

- Conocer el estado de la tramitación de su denuncia y los resultados de la investigación.

5.1.6 Medidas de protección de la persona informante y prohibición de represalias

MEDIDAS DE PROTECCIÓN

- En primer lugar, indicar que las personas informantes que deseen dar traslado de información mediante el canal interno de comunicación de TOGAMA, S.A. contarán con una serie de medidas de protección, siempre que revelen infracciones previstas en la ley 2/2023, de 20 de febrero siempre que concurran las siguientes circunstancias:

- Tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación o revelación, aun cuando no aporten pruebas concluyentes, y que la citada información entra dentro del ámbito de aplicación de la citada ley.

- La comunicación o revelación se haya realizado conforme a los requerimientos previstos en la citada ley.

Quedan expresamente **excluidos** de la protección prevista en la ley 2/2023, de 20 de febrero aquellas personas que comuniquen o revelen:

- Información contenida en comunicaciones que hayan sido inadmitidas por algún canal interno de información o por alguna de las causas previstas en la legislación.

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

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

- Informaciones que se refieran a acciones u omisiones no comprendidas en el alcance de la legislación.

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

Las personas que informen ante las instituciones, órganos u organismos pertinentes de la Unión Europea infracciones que entren en el ámbito de aplicación de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, tendrán derecho a protección con arreglo a lo dispuesto en la ley 2/2023, de 20 de febrero, en las mismas condiciones que una persona que haya informado por canales externos.

CONCEPTO DE REPRESALIAS

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 dentro del ámbito de aplicación del presente procedimiento de gestión de informaciones.
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.

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

1. **Suspensión del contrato de trabajo, despido o extinción de la relación laboral**, 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 la persona trabajadora tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido; salvo que estas medidas se lleven a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral.

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

3. **Evaluación o referencias negativas** respecto al desempeño laboral o profesional.

4. **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.

5. Denegación o anulación de una licencia o permiso.

6. Denegación de formación.

7. Discriminación, o trato desfavorable o injusto.

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, 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 a la persona perjudicada.

MEDIDAS DE PROTECCIÓN A LA PERSONA INFORMANTE FRENTE A REPRESALIAS

Dentro de las medidas de protección frente a represalias a la persona informante cabe destacar que no se considerará que las personas que comuniquen información sobre las acciones u omisiones recogidas en este procedimiento o en la legislación vigente o que hagan una revelación pública haya infringido ninguna restricción de revelación de información, y aquellas no incurrirán en responsabilidad de ningún tipo en relación con dicha comunicación o revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública de dicha información era necesaria para revelar una acción u omisión. Esta medida no afectará a las responsabilidades de carácter penal.

Lo previsto en el párrafo anterior se extiende a la comunicación de informaciones realizadas por los y las representantes de las personas trabajadoras, aunque se encuentren sometidas a obligaciones legales de sigilo

o de no revelar información reservada. Todo ello sin perjuicio de las normas específicas de protección aplicables conforme a la normativa laboral.

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

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

En los procedimientos ante un órgano jurisdiccional u otra autoridad relativos a los perjuicios sufridos por las personas informantes, una vez que la persona informante haya demostrado razonablemente que ha comunicado o ha hecho una revelación pública de conformidad con la legislación vigente en materia del procedimiento de gestión de informaciones y que ha sufrido un perjuicio, se presumirá que el perjuicio se produjo como represalia por informar o por hacer una revelación pública. En tales casos, corresponderá a la persona que haya tomado la medida perjudicial probar que esa medida se basó en motivos debidamente justificados no vinculados a la comunicación o revelación pública.

En los procesos judiciales, incluidos los relativos a difamación, violación de derechos de autor, vulneración de secreto, infracción de las normas de protección de datos, revelación de secretos empresariales, o a solicitudes de indemnización basadas en el derecho laboral o estatutario, las personas no incurrirán en responsabilidad de ningún tipo como consecuencia de comunicaciones o de revelaciones públicas protegidas por la legislación vigente. Dichas personas tendrán derecho a alegar en su descargo y en el marco de los referidos procesos judiciales, el haber comunicado o haber hecho una revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública era necesaria para poner de manifiesto una infracción en virtud de la ley 2/2023, del 20 de febrero.

MEDIDAS DE APOYO A LA PERSONA INFORMANTE

Las personas que comuniquen o revelen infracciones materia del presente procedimiento accederán a las medidas de apoyo siguientes:

- Información y asesoramiento, que sean fácilmente accesibles, sobre los procedimientos y recursos disponibles, protección frente a represalias y derechos de la persona afectada. Será responsabilidad de **TOGAMA, S.A.** dar comunicación sobre esta materia.

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.

MEDIDAS DE PROTECCIÓN A LAS PERSONAS AFECTADAS

Durante la tramitación del expediente las personas afectadas por la comunicación tendrán derecho a la **presunción de inocencia**, al **derecho de defensa** y al **derecho de acceso al expediente** salvo revelación de datos personales de la información recibida en el canal interno de información, así como a la misma

protección establecida para las personas informantes, preservándose su identidad y garantizando la confidencialidad de los hechos y datos del procedimiento.

5.1.7 Régimen sancionador

El ejercicio de la potestad sancionadora en el ámbito de la ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción se llevará a cabo conforme a los principios y con sujeción a las reglas de procedimiento previstas en la Ley 40/2015, de 1 de octubre, y la Ley 39/2015, de 1 de octubre.

Le corresponde el ejercicio de la potestad sancionadora a la Autoridad Independiente de Protección del Informante, A.A.I., y a los órganos competentes de las comunidades autónomas, sin perjuicio de las facultades disciplinarias que en el ámbito interno de cada organización pudieran tener los órganos competentes.

La Autoridad Independiente de Protección del Informante, A.A.I. será competente respecto de las infracciones cometidas en el ámbito del **sector público estatal**. También será competente respecto a las infracciones cometidas en el ámbito del **sector privado** en todo el territorio, siempre que la normativa autonómica correspondiente no haya atribuido esta competencia a los organismos competentes de las respectivas comunidades autónomas. La competencia para la imposición de sanciones derivadas de los procedimientos competencia de la Autoridad Independiente de Protección del Informante, A.A.I. corresponderá a la persona titular de su presidencia.

Los órganos competentes de las comunidades autónomas lo serán exclusivamente respecto de las infracciones cometidas en el ámbito del sector público autonómico y local del territorio de la correspondiente comunidad autónoma. La normativa autonómica podrá prever que dichos órganos sean competentes respecto de las infracciones cometidas en el ámbito del sector privado cuando afecten solamente a su ámbito territorial.

SUJETOS RESPONSABLES

Estarán sujetas al régimen sancionador previsto las personas físicas y jurídicas que realicen cualquiera de las actuaciones descritas como infracciones en el artículo 63 de la ley 2/2023, de 20 de febrero.

Cuando la comisión de la infracción se atribuya a un órgano colegiado la responsabilidad será exigible en los términos que señale la resolución sancionadora. Quedarán exentas de responsabilidad aquellas personas miembro que no hayan asistido por causa justificada a la reunión en que se adoptó el acuerdo o que hayan votado en contra del mismo.

La exigencia de responsabilidades derivada de las infracciones tipificadas se extenderá a las personas responsables incluso aunque haya desaparecido su relación o cesado en su actividad en o con la entidad respectiva.

INFRACCIONES

Tendrán la consideración de **infracciones muy graves** las siguientes acciones u omisiones dolosas:

- Cualquier actuación que suponga una efectiva limitación de los derechos y garantías previstos en el presente procedimiento introducida a través de contratos o acuerdos a nivel individual o colectivo y en general cualquier intento o acción efectiva de obstaculizar la presentación de comunicaciones o de impedir, frustrar o ralentizar su seguimiento, incluida la aportación de información o documentación falsa por parte de los requeridos para ello.

- La adopción de cualquier represalia derivada de la comunicación frente a las personas informantes o las demás personas incluidas en el ámbito de protección establecido en el presente procedimiento.

- Vulnerar las garantías de confidencialidad y anonimato previstas en este procedimiento y de forma particular cualquier acción u omisión tendente a revelar la identidad de la persona informante cuando esta haya optado por el anonimato, aunque no se llegue a producir la efectiva revelación de la misma.

- Vulnerar el deber de mantener secreto sobre cualquier aspecto relacionado con la información.

- La comisión de una infracción grave cuando la persona autora hubiera sido sancionada mediante resolución firme por dos infracciones graves o muy graves en los dos años anteriores a la comisión de la infracción, contados desde la firmeza de las sanciones.

- Comunicar o revelar públicamente información a sabiendas de su falsedad.

- Incumplimiento de la obligación de disponer de un Sistema interno de información en los términos exigidos en esta ley.

Tendrán la consideración de **infracciones graves** las siguientes acciones u omisiones:

- Cualquier actuación que suponga limitación de los derechos y garantías previstos en este procedimiento o cualquier intento o acción efectiva de obstaculizar la presentación de informaciones o de impedir, frustrar o ralentizar su seguimiento que no tenga la consideración de infracción muy grave conforme al apartado 1.

- Vulnerar las garantías de confidencialidad y anonimato previstas en esta ley cuando no tenga la consideración de infracción muy grave.

- Vulnerar el deber de secreto en los supuestos en que no tenga la consideración de infracción muy grave.

- Incumplimiento de la obligación de adoptar las medidas para garantizar la confidencialidad y secreto de las informaciones.

- La comisión de una infracción leve cuando la persona autora hubiera sido sancionada por dos infracciones leves, graves o muy graves en los dos años anteriores a la comisión de la infracción, contados desde la firmeza de las sanciones.

Tendrán la consideración de **infracciones leves** las siguientes acciones u omisiones:

- Remisión de información de forma incompleta, de manera deliberada por parte de la Responsable del Sistema interno de Información a la Autoridad, o fuera del plazo concedido para ello.

- Incumplimiento de la obligación de colaboración con la investigación de informaciones.

- Cualquier incumplimiento de las obligaciones previstas en esta ley que no esté tipificado como infracción muy grave o grave.

SANCIONES

La comisión de infracciones previstas en la ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción llevará aparejada la imposición de las siguientes **multas**:

- Si son personas físicas las responsables de las infracciones, serán multadas con una cuantía de:
  - 1.001 hasta 10.000 euros por la comisión de **infracciones leves**
  - 10.001 hasta 30.000 euros por la comisión de **infracciones graves**
  - 30.001 hasta 300.000 euros por la comisión de **infracciones muy graves**.

- Si son personas jurídicas serán multadas con una cuantía:
  - Hasta 100.000 euros en caso de **infracciones leves**.
  - Entre 100.001 y 600.000 euros en caso de **infracciones graves**.
  - Entre 600.001 y 1.000.000 de euros en caso de **infracciones muy graves**.

Adicionalmente, en el caso de infracciones muy graves, la Autoridad Independiente de Protección del Informante, A.A.I., podrá acordar:

- La amonestación pública.

- La prohibición de obtener subvenciones u otros beneficios fiscales durante un plazo máximo de cuatro años.

- La prohibición de contratar con el sector público durante un plazo máximo de tres años de conformidad con lo previsto en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

Las sanciones por infracciones muy graves de cuantía igual o superior a 600.001 euros impuestas a entidades jurídicas podrán ser publicadas en el «Boletín Oficial del Estado», tras la firmeza de la resolución en vía administrativa. La publicación deberá contener, al menos, información sobre el tipo y naturaleza de la infracción y, en su caso, la identidad de las personas responsables de las mismas de acuerdo con la normativa en materia de protección de datos.

Para la graduación de las infracciones se pueden tener en cuenta los criterios siguientes:

- La reincidencia, siempre que no hubiera sido tenido en cuenta previamente.

- La entidad y persistencia temporal del daño o perjuicio causado.

- La intencionalidad y culpabilidad de la persona autora.

- El resultado económico del ejercicio anterior de la persona infractora.
- La circunstancia de haber procedido a la subsanación del incumplimiento que dio lugar a la infracción por propia iniciativa.
- La reparación de los daños o perjuicios causados.
- La colaboración con la Autoridad Independiente de Protección del Informante, A.A.I., u otras autoridades administrativas.

5.1.8 Disposiciones finales

La persona responsable del sistema interno de información de **TOGAMA, S.A.** revisarán sus procedimientos de recepción y seguimiento de informaciones al menos una vez cada al año, incorporando actuaciones y buenas prácticas con la finalidad de que sirvan con la mayor eficacia a los fines para los que fueron creados.

Todos los sujetos obligados a disponer de un canal interno de informaciones, con independencia de que formen parte del sector público o del sector privado, deberán contar con un **libro-registro de las informaciones recibidas y de las investigaciones internas** a que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad previstos en esta ley.

Este registro no será público y únicamente a petición razonada de la Autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquella, podrá accederse total o parcialmente al contenido del referido registro.

Los datos personales relativos a las informaciones recibidas y a las investigaciones internas a que se refiere el apartado anterior sólo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con la legislación. En ningún caso podrán conservarse los datos por un período superior a diez años. **TOGAMA, S.A.** conservará los datos por un periodo de cinco años, por si se necesita presentar la información ante la autoridad competente o ante el Ministerio Fiscal.

La regulación y procedimientos establecidos en este procedimiento no impiden, en ningún momento, si pueden promover y tramitar cualquier otra acción para exigir responsabilidades administrativas, sociales, civiles o penales que, en su caso, correspondan.

- Tanto la dirección de la empresa como la representación del personal deberán informar y dar asesoramiento a las personas trabajadores que lo requieran sobre esta temática.

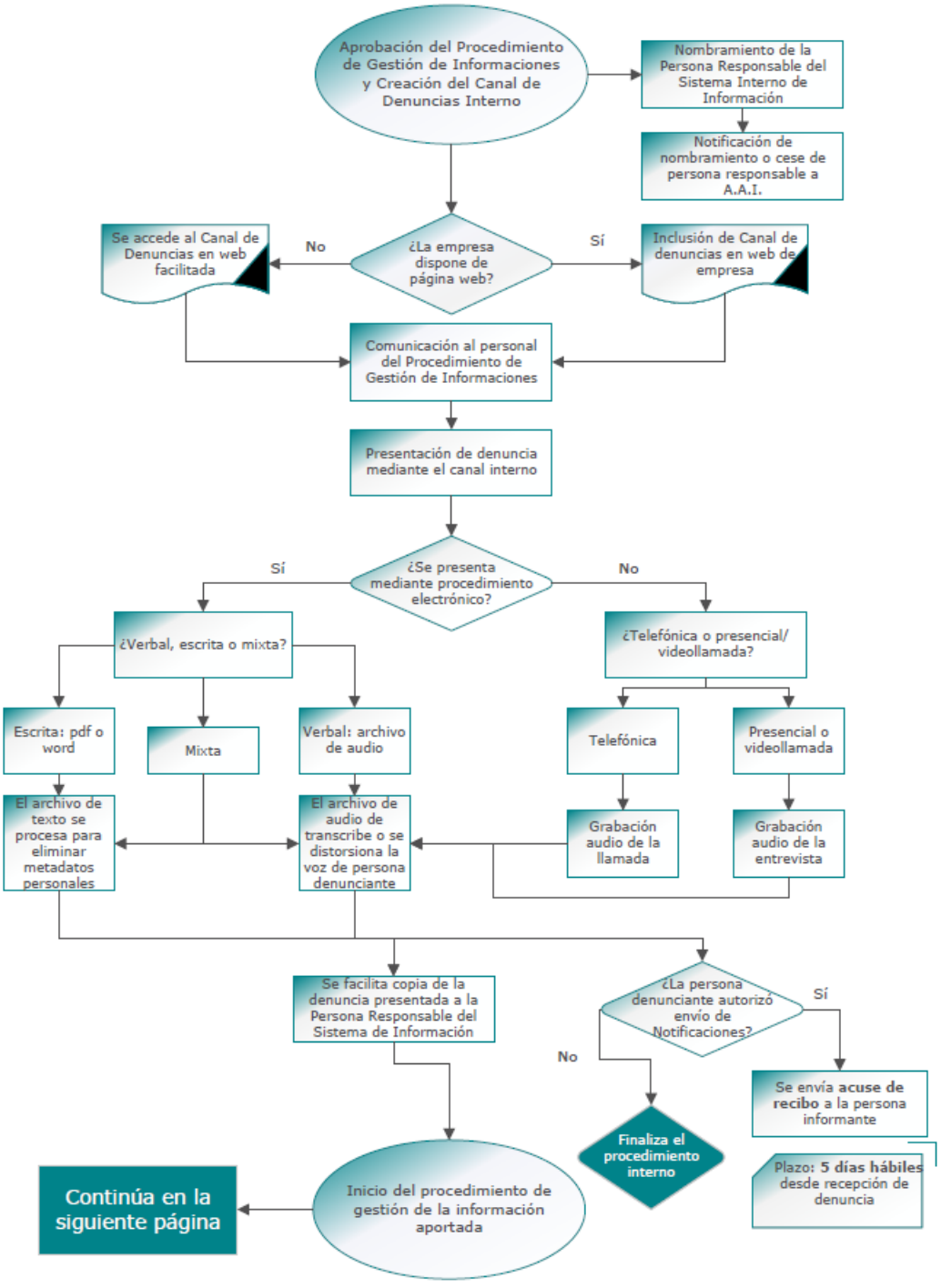
- El contenido de este procedimiento es obligatorio, entrando en vigor a partir de su firma.

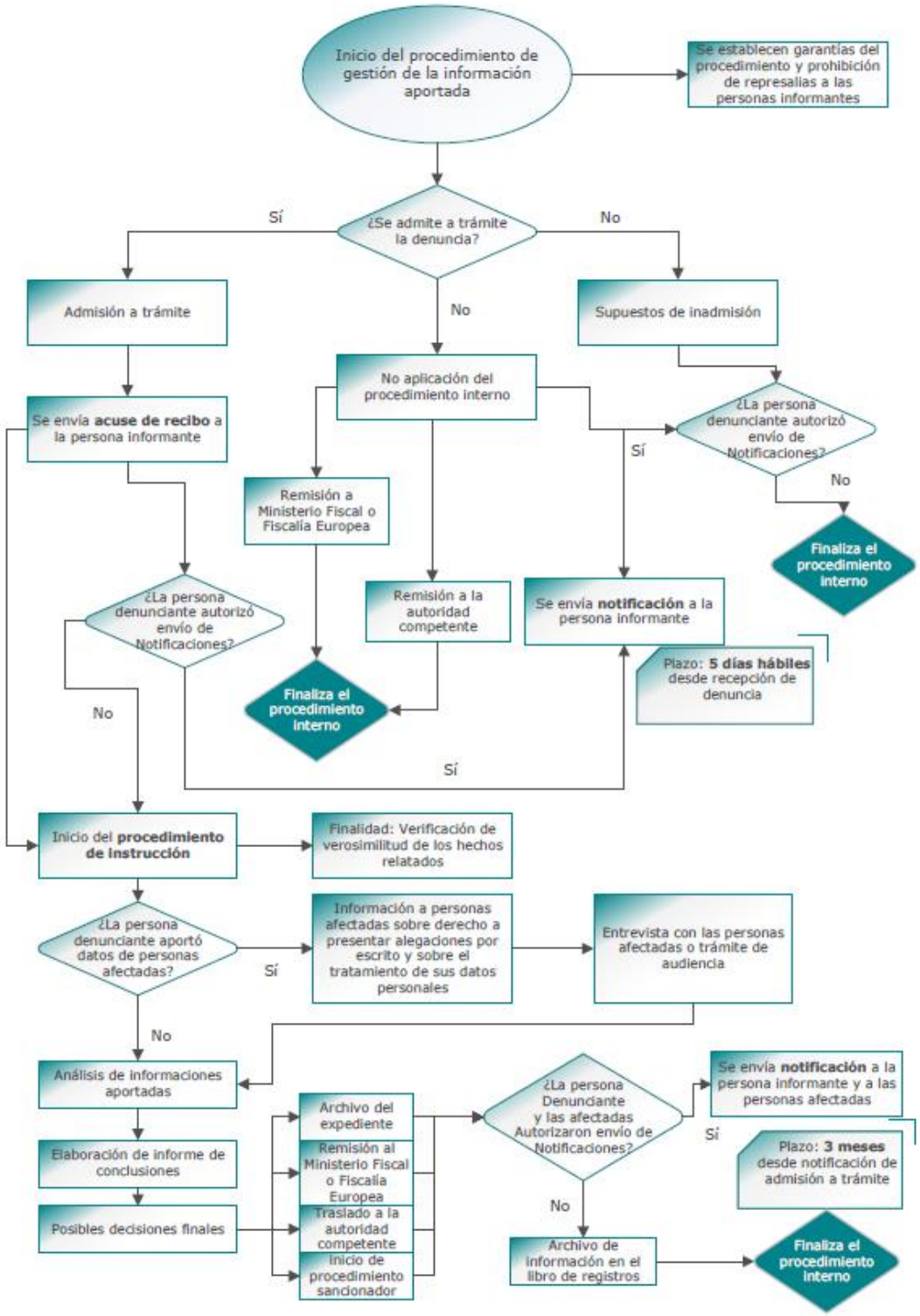
En CASTELLÓN, a 22/09/2023.

Firmas (Indicar nombre, apellidos y DNI)

6. Anexos

Esquema del procedimiento




Inicio del procedimiento de gestión de la información aportada
Se establecen garantías del procedimiento y prohibición de represalias a las personas informantes
¿Se admite a trámite la denuncia?
Sí
No
Admisión a trámite
No
Supuestos de inadmisión
No aplicación del procedimiento interno
Se envía acuse de recibo a la persona informante
¿La persona denunciante autorizó envío de Notificaciones?
Sí
No
Finaliza el procedimiento interno
Remisión a Ministerio Fiscal o Fiscalía Europea
Remisión a la autoridad competente
Se envía notificación a la persona informante
Plazo: 5 días hábiles desde recepción de denuncia
¿La persona denunciante autorizó envío de Notificaciones?
No
Finaliza el procedimiento interno
Sí
Inicio del procedimiento de instrucción
Finalidad: Verificación de verosimilitud de los hechos relatados
¿La persona denunciante aportó datos de personas afectadas?
Sí
Información a personas afectadas sobre derecho a presentar alegaciones por escrito y sobre el tratamiento de sus datos personales
Entrevista con las personas afectadas o trámite de audiencia
No
Análisis de informaciones aportadas
Elaboración de informe de conclusiones
Posibles decisiones finales
Archivo del expediente
Remisión al Ministerio Fiscal o Fiscalía Europea
Traslado a la autoridad competente
Inicio de procedimiento sancionador
¿La persona Denunciante y las afectadas Autorizaron envío de Notificaciones?
Se envía notificación a la persona informante y a las personas afectadas
Sí
Plazo: 3 meses desde notificación de admisión a trámite
No
Archivo de información en el libro de registros
Finaliza el procedimiento interno

Modelo de aceptación del cargo de persona Responsable del Sistema Interno de Informaciones

Don / Doña _____, con DNI: _____, habiendo sido designado/a por **TOGAMA, S.A.** para desempeñar el cargo de "*Responsable del Sistema interno de Informaciones*" con arreglo a lo establecido en el Procedimiento de Gestión de Informaciones de la empresa,

ME COMPROMETO

- A asumir las funciones y desempeñar la labor indicada para esta figura en dicho Procedimiento interno siguiendo los preceptos de independencia y autonomía respecto al resto de órganos de **TOGAMA, S.A.**.
- A actuar con la máxima diligencia posible para discernir sobre los hechos denunciados y actuar sin prejuicios con ninguna de las personas implicadas.
- A respetar la confidencialidad, privacidad, intimidad e imparcialidad de las partes a lo largo de las diferentes fases de los procesos en los que pudiera intervenir.

De forma más concreta, **MANIFIESTO** mi compromiso a cumplir con las siguientes obligaciones:

- Informar con claridad a todo el personal de la empresa, así como a empresas proveedoras, contratistas o subcontratistas de nuestro canal interno de denuncias, así como a resolver dudas sobre la correcta utilización del mismo.
- Enviar los acuses de recibo y notificaciones pertinentes a las personas informantes y afectadas del avance de las investigaciones y de los resultados finales de las mismas, siempre y cuando esas personas no hayan renunciado a su derecho a ser notificadas.
- Ceñirme a los tiempos y plazos establecidos para dar respuesta a las actuaciones de investigación establecidas en el procedimiento.
- Garantizar la dignidad de las personas y su derecho a la intimidad y presunción de inocencia y honor a lo largo de todas las etapas del procedimiento, así como la prohibición de represalias a las personas informantes.
- Garantizar el tratamiento reservado y la más absoluta discreción en relación con la información sobre las situaciones que pudieran ser constitutivas de delito por acciones u omisiones
- Garantizar la más estricta confidencialidad y reserva sobre el contenido de las denuncias presentadas, resueltas o en proceso de investigación de las que tenga conocimiento, así como velar por el cumplimiento de la prohibición de divulgar o transmitir cualquier tipo de información por parte del resto de las personas que intervengan en los procedimientos.
- Remisión de la información al Ministerio Fiscal o Fiscalía Europea con carácter inmediato si los hechos pueden ser indiciariamente constitutivos de delito, así como a las autoridades competentes en caso de que se entreguen denuncias que excedan el ámbito de aplicación del presente procedimiento.

Asimismo, declaro que he sido informado por **TOGAMA, S.A.**, de la responsabilidad disciplinaria en que podría incurrir por incumplimiento de las obligaciones anteriormente expuestas.

En VILLARREAL, a ____ de _____ de _____.

Firmado:

Modelo de compromiso de confidencialidad

Don / Doña _____, con DNI: _____, habiendo sido solicitado/a por la persona Responsable del Sistema Interno de Informaciones de **TOGAMA, S.A.** para intervenir como persona informante / persona afectada / testigo/a de los hechos denunciados, ejerciendo mi derecho a presentar alegaciones por escrito o a personarme en las entrevistas que el procedimiento requiera para su buen funcionamiento

ME COMPROMETO

A respetar la confidencialidad, privacidad, intimidad, presunción de inocencia y honor e imparcialidad de las partes a lo largo de las diferentes fases del proceso.

Por lo tanto, y de forma más concreta, **MANIFIESTO** mi compromiso a cumplir con las siguientes obligaciones:

- Garantizar la dignidad de las personas y su derecho a la intimidad y presunción de inocencia y honor a lo largo de todas las etapas del procedimiento, así como la prohibición de represalias a las personas informantes.
- Garantizar el tratamiento reservado y la más absoluta discreción en relación con la información sobre las situaciones que pudieran ser constitutivas de delito por acciones u omisiones.
- Garantizar la prohibición de represalias contra las personas informantes, tal como se describe en el Procedimiento de Gestión de Informaciones.
- Garantizar la más estricta confidencialidad y reserva sobre el contenido de las denuncias presentadas, resueltas o en proceso de investigación de las que tenga conocimiento, así como velar por el cumplimiento de la prohibición de divulgar o transmitir cualquier tipo de información por parte del resto de las personas que intervengan en los procedimientos.

Asimismo, declaro que he sido informado por **TOGAMA, S.A.**, de la responsabilidad disciplinaria en que podría incurrir por incumplimiento de las obligaciones anteriormente expuestas, así como el conocimiento acerca de las medidas de protección descritas y las garantías del procedimiento.

En VILLARREAL, a ____ de _____ de _____.

Firmado:

Modelo de denuncia

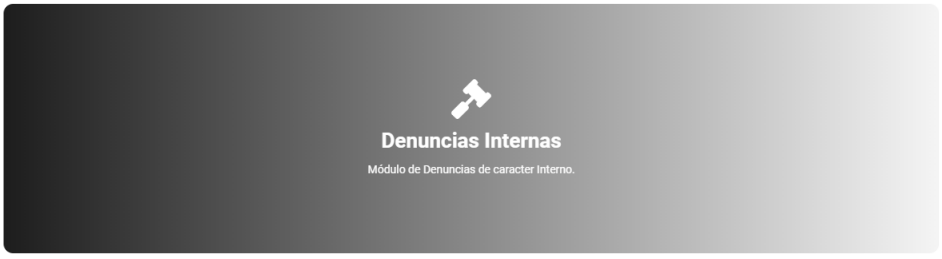
TOGAMA
MORE THAN MOSAIC

+34 988 80 86 64
denuncias@ingade.es

Bienvenida/o al Canal interno de Denuncias de **TOGAMA S.A.**, Le recordamos que puede presentar sus denuncias o aportar informaciones tanto de forma anónima como identificada sobre las temáticas que podrá ver a continuación.

Tanto la persona informante como las afectadas por la denuncia tienen derecho a la preservación de su identidad en los términos previstos en la Ley 2/2023, de 20 de febrero. Además, las personas informantes cuentan con derechos entre los que se incluye la **prohibición de represalias**.

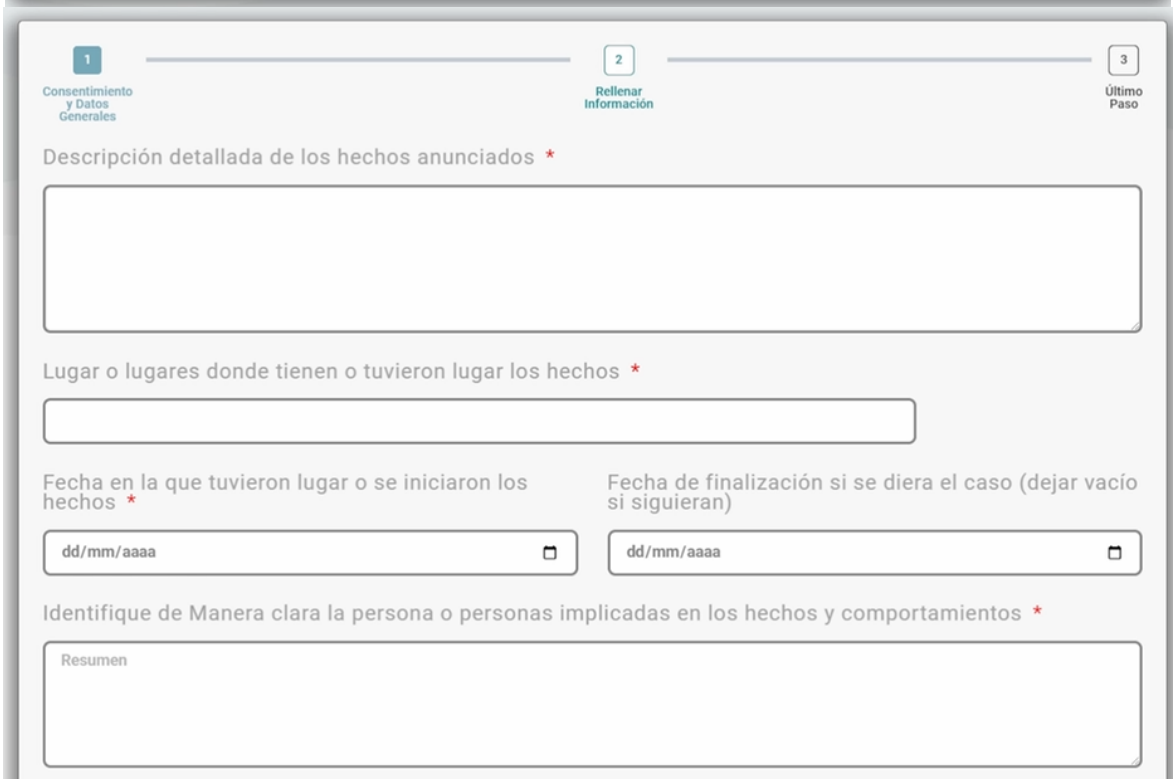
Recuerde que comunicar o revelar públicamente información a sabiendas de su falsedad se considera infracción muy grave y que la ley prevé multa desde **30.001 hasta 300.000€** para las personas físicas que las cometan. Puede consultar nuestra política, así como el resto de aspectos técnicos en el **Procedimiento de Gestión de Informaciones.**

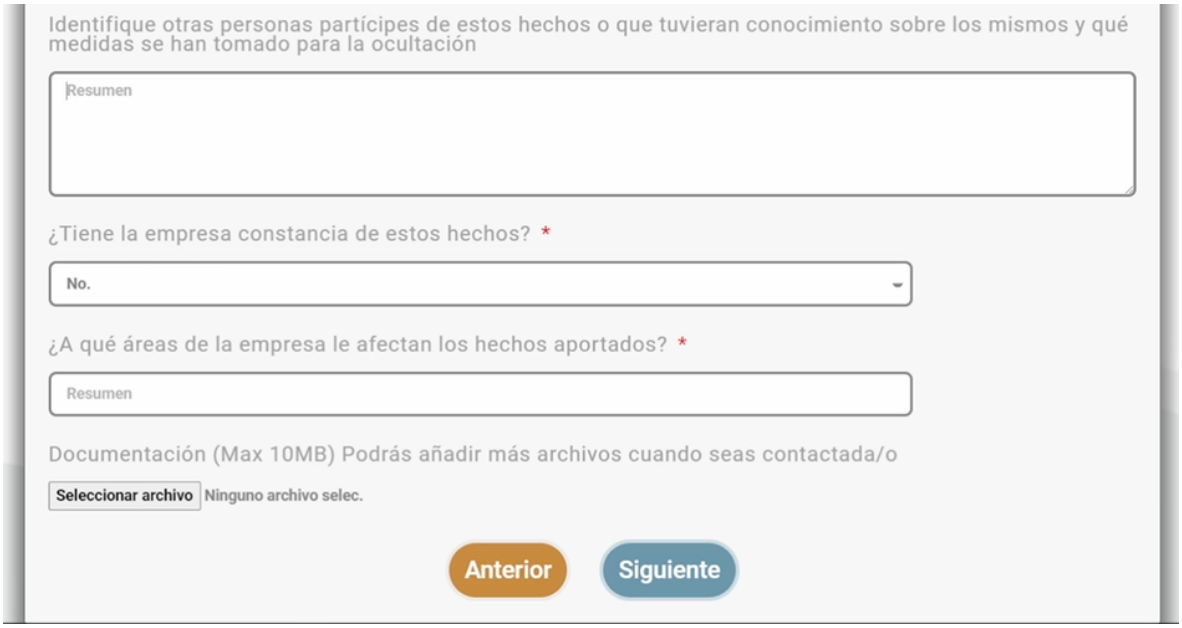


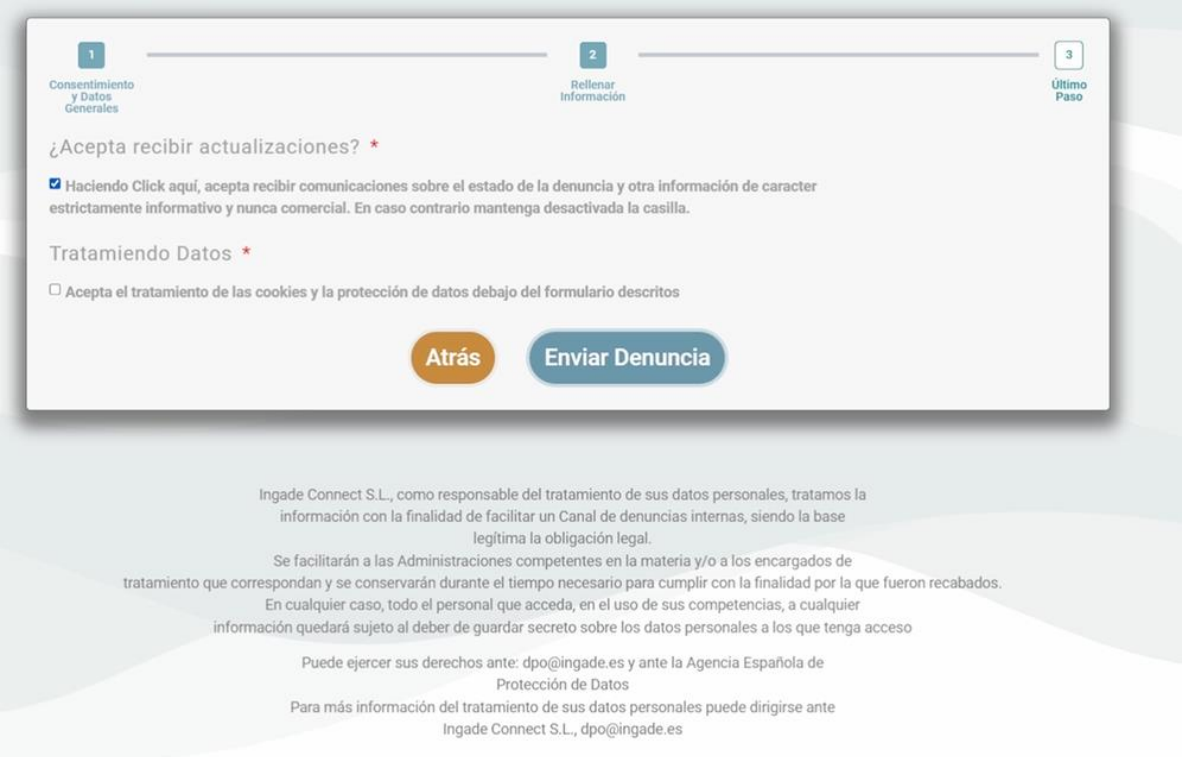
Le recordamos que puede ejercer sus derechos de presentación de información a través de los canales externos de denuncias e información habilitados ante la autoridad **Independiente de Protección del Informante**, surgida a raíz de la **Ley 2/2023, de 20 de febrero**, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, transposición 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, o ante las autoridades u órganos autonómicos correspondientes. Así mismo, le informamos que las decisiones tomadas tras la investigación pertinente pueden ser remitidas al Ministerio Fiscal (si los hechos pueden ser indiciariamente constitutivos de delito), a la Fiscalía Europea (si los hechos afectan a intereses financieros de la Unión Europea) o autoridad, entidad u organismo competente para su tramitación. El plazo máximo para resolver desde que la información entra en registro será de 3 meses.

Le recordamos que, si hace uso de nuestro canal interno de información se reservará su entidad como persona informante o puede ser realizada de forma totalmente anónima si así lo prefiere, siempre con las garantías de protección frente a represalias.


1
Consentimiento y Datos Generales
2
Rellenar Información
3
Último Paso
¿Confirmas que conoces los otros medios de comunicación descritos arriba y quieres seguir? *
Nombre (Opcional)
Nombre Apellido1 Apellido2
Teléfono (Opcional)
+34 667 788 599
Email (Necesario para actualizaciones)
nombre@correo.com
Identifique su relación con la organización *
Empresa Proveedora
Comenzar


1
Consentimiento y Datos Generales
2
Rellenar Información
3
Último Paso
Descripción detallada de los hechos anunciados *
Lugar o lugares donde tienen o tuvieron lugar los hechos *
Fecha en la que tuvieron lugar o se iniciaron los hechos *
dd/mm/aaaa
Fecha de finalización si se diera el caso (dejar vacío si siguieran)
dd/mm/aaaa
Identifique de Manera clara la persona o personas implicadas en los hechos y comportamientos *
Resumen


Identifique otras personas partícipes de estos hechos o que tuvieran conocimiento sobre los mismos y qué medidas se han tomado para la ocultación
Resumen
¿Tiene la empresa constancia de estos hechos? *
No.
¿A qué áreas de la empresa le afectan los hechos aportados? *
Resumen
Documentación (Max 10MB) Podrás añadir más archivos cuando seas contactada/o
Seleccionar archivo
Ninguno archivo selec.
Anterior
Siguiente


1
Consentimiento y Datos Generales
2
Rellenar Información
3
Último Paso
¿Acepta recibir actualizaciones? *
Haciendo Click aquí, acepta recibir comunicaciones sobre el estado de la denuncia y otra información de caracter estrictamente informativo y nunca comercial. En caso contrario mantenga desactivada la casilla.
Tratamiendo Datos *
Acepta el tratamiento de las cookies y la protección de datos debajo del formulario descritos
Atrás
Enviar Denuncia
Ingade Connect S.L., como responsable del tratamiento de sus datos personales, tratamos la información con la finalidad de facilitar un Canal de denuncias internas, siendo la base legítima la obligación legal.
Se facilitarán a las Administraciones competentes en la materia y/o a los encargados de tratamiento que correspondan y se conservarán durante el tiempo necesario para cumplir con la finalidad por la que fueron recabados.
En cualquier caso, todo el personal que acceda, en el uso de sus competencias, a cualquier información quedará sujeto al deber de guardar secreto sobre los datos personales a los que tenga acceso
Puede ejercer sus derechos ante: dpo@ingade.es y ante la Agencia Española de Protección de Datos
Para más información del tratamiento de sus datos personales puede dirigirse ante Ingade Connect S.L., dpo@ingade.es

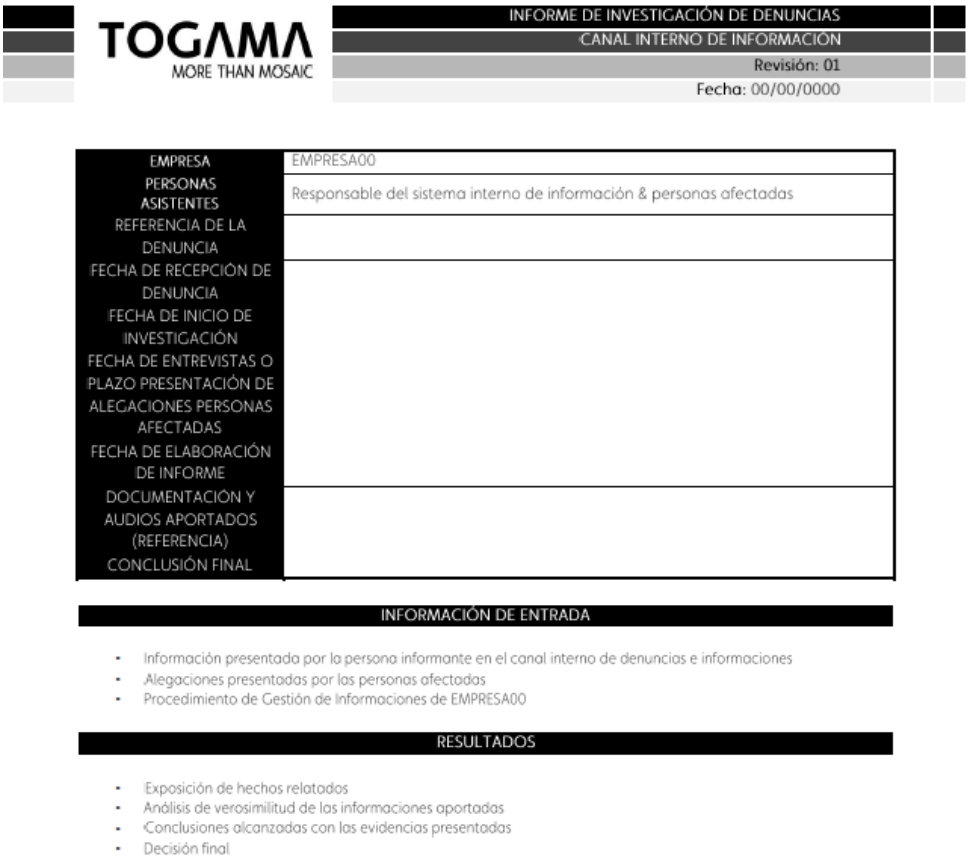
Modelo de libro-registro de la información recibida e investigaciones internas

LIBRO – REGISTRO DE LA INFORMACIÓN RECIBIDA EN EL CANAL*							
Fecha denuncia	Hora denuncia	Anónima o identificada	¿Acepta notificaciones?	Anexos	Estado procedimiento	Cierre de actuaciones	Personas afectadas

*Notas:

- Fecha y hora de la denuncia se registran para la trazabilidad
- Anónima (sin datos de contacto) o identificada (facilita datos de contacto pero se le asigna un código identificativo
- Estado del procedimiento: puede contemplar las siguientes etapas:
    - Denuncia recibida
    - Admitida a trámite
    - En investigación
    - Elaboración de informe
    - Toma de decisiones
- Cierre de actuaciones: puede contemplar las siguientes etapas
    - Inadmisión a trámite
    - Archivada
    - Procedimiento sancionador
    - Enviada a Ministerio Fiscal/Fiscalía Europea
    - Derivada a autoridad competente

Formato de informe de investigación



TOGAMA
MORE THAN MOSAIC

INFORME DE INVESTIGACIÓN DE DENUNCIAS
CANAL INTERNO DE INFORMACIÓN
Revisión: 01
Fecha: 00/00/0000

EMPRESA	EMPRESA00
PERSONAS ASISTENTES	Responsable del sistema interno de información & personas afectadas
REFERENCIA DE LA DENUNCIA	
FECHA DE RECEPCIÓN DE DENUNCIA	
FECHA DE INICIO DE INVESTIGACIÓN	
FECHA DE ENTREVISTAS O PLAZO PRESENTACIÓN DE ALEGACIONES PERSONAS AFECTADAS	
FECHA DE ELABORACIÓN DE INFORME	
DOCUMENTACIÓN Y AUDIOS APORTADOS (REFERENCIA)	
CONCLUSIÓN FINAL	

INFORMACIÓN DE ENTRADA

- Información presentada por la persona informante en el canal interno de denuncias e informaciones
- Alegaciones presentadas por las personas afectadas
- Procedimiento de Gestión de Informaciones de EMPRESA00

RESULTADOS

- Exposición de hechos relatados
- Análisis de verosimilitud de las informaciones aportadas
- Conclusiones alcanzadas con las evidencias presentadas
- Decisión final

Página 1 de 3

INFORMACIÓN DE ENTRADA

El **objeto** del presente informe es Realizar la investigación pertinente tras la recepción de información en el canal interno de denuncias de EMPRESA00. En primer lugar se analiza la información aportada para concluir si aplica o no la admisión a trámite según el procedimiento de gestión de información de la empresa. En el caso que nos ocupa se ha admitido a trámite, en caso contrario no se levantaría informe. Pasamos a detallar la documentación e información aportada para su posterior análisis

1) Información presentada por la persona informante en el canal interno de denuncias e informaciones

Se ha recibido la siguiente documentación e información:

-
-
-

2) Alegaciones presentadas por las personas afectadas

Las personas afectadas han presentado las siguientes alegaciones:

-
-
-

Con las informaciones recibidas por todas las partes implicadas se procede al análisis de resultados

RESULTADOS

3) Exposición de hechos relatados

Como persona responsable del sistema interno de información, tras la lectura y análisis de las informaciones presentadas puedo afirmar que los hechos que se relatan son los siguientes:

-
-
-

4) Análisis de verosimilitud de las informaciones aportadas

Tras la exposición de hechos, se analiza la información aportada, de la que se puede comprobar que existe verosimilitud en las informaciones ___, ___ y ___. No obstante, se aprecia falta de verosimilitud en lo concerniente a _____ y _____.

5) Conclusiones alcanzadas

Se presentan como conclusiones del presente informe las siguientes:

-
-
-

6) Decisión final

En base a toda la exposición de hechos relatada y al análisis efectuado, se ha tomado la decisión de tomar como decisión final:

- Archivo del expediente y notificación a las personas informantes y afectadas.
- Remisión al Ministerio Fiscal o Fiscalía Europea, al apreciarse indicios de hechos que pueden revestir el carácter de delito.
- Traslado a la autoridad competente para su tramitación, siendo conscientes de que excede nuestras competencias.
- Adopción de acuerdo de inicio de procedimiento sancionador

Hoja formativa: evidencia de conocimiento del personal

El presente registro constata que las personas trabajadoras pertenecientes a **TOGAMA, S.A.** conocen la existencia y el contenido del PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES y CANAL INTERNO DE INFORMACIÓN / DENUNCIAS de la empresa.

FECHA	NOMBRE Y APELLIDOS PERSONA TRABAJADORA	DNI	FIRMA PERSONA TRABAJADORA