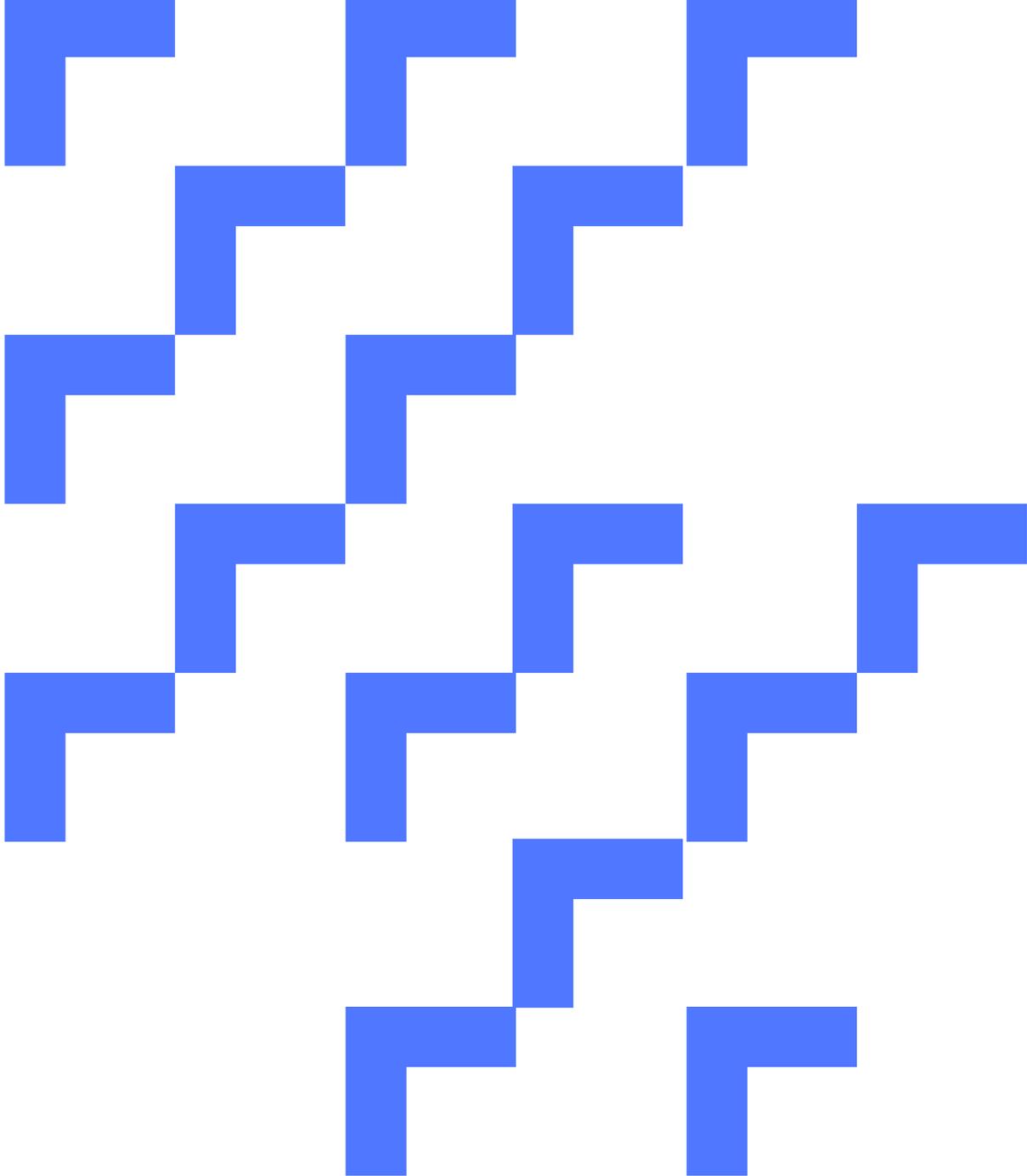


Cumpliendo con la Ley 2/23: 13 preguntas recurrentes

Aspectos jurídicos
importantes: análisis
detallado.

ANEXO



GlobalSuite
SOLUTIONS

Índice

• Denuncia por voz	4
• Acceso al expediente	5
• Metadatos	6
• Derecho a no autoinculparse	7
• Delitos comprendidos en el alcance de la norma	7
• Sujetos protegidos por la norma	7
• La relación sobre el tratamiento confidencial de las informaciones con el derecho del investigado a conocer los hechos que se le atribuyen para poder defenderse	8
• ¿La norma exige la obligatoriedad de implementar un canal de informaciones que implique la recepción de informaciones verbales?	9
• Plazos de conservación	11

ASPECTOS JURÍDICOS IMPORTANTES: ANÁLISIS DETALLADO

DENUNCIAS POR VOZ

Con carácter general y como cuestión antecedente, las comunicaciones pueden llevarse a cabo de forma anónima o con reserva de identidad del informante, y sobre su forma la norma permite las opciones de comunicar por escrito o verbalmente, o de ambos modos -artículo 5.2 de la Ley del Informante-, además de estar diseñados, establecidos y gestionados de forma segura. La funcionalidad de distorsión de voz tiene sentido para el caso de denuncias anónimas pero la ley da varias opciones de comunicación cuando se refiere a comunicar por "escrito" o "verbal" o "de ambas formas" y no especifica que tenga que ser a elección del informante "(...) El canal interno deberá permitir realizar comunicaciones por escrito o verbalmente, o de las dos formas.

La información se podrá realizar bien por escrito, a través de correo postal o a través de cualquier medio electrónico habilitado al efecto, o verbalmente, por vía telefónica o a través de sistema de mensajería de voz (...).

El informante, en el supuesto de comunicar con reserva de identidad, una vez realizada la comunicación incluidas las realizadas a través de reunión presencial, telefónicamente o mediante sistema de mensajería de voz, éstas deberán estar documentadas de alguna de las maneras, previo consentimiento del informante:

- i. Mediante una grabación de la conversación en formato seguro, duradero y accesible.
- ii. O a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla. Se entiende que el consentimiento se refiere a la elección de cualquiera de las dos vías, no a documentar en sí la comunicación verbal.

El problema que puedo observar:

- i. es el supuesto de un informante que se identifique, realice una comunicación verbal pero que luego quiera ser anónimo, -artículo 7.3 de la Ley del Informante que conmina a que los canales internos deberán permitir la presentación y posterior tramitación de comunicaciones anónimas-.
- ii. como el canal está habilitado para realizar comunicaciones verbales y escritas, entiendo que debería dotar de las mismas garantías a las comunicaciones que se realizaran por voz de forma anónima.



Ley 2/2023 -en lo sucesivo, la Ley-, indica en el artículo 39 de la Ley sobre las medidas para la protección de las personas afectadas en la que dice expresamente (...) 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 en los términos regulados en esta ley, así como a la misma protección establecida para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento. Si nos remitimos a “los términos regulados en esta ley” del artículo 39 debemos acudir al artículo 9.2.f) que regula el procedimiento de gestión de informaciones e indica que la persona afectada o investigada tendrá derecho a ser informada de las acciones u omisiones que se le atribuyen, a ser oída en cualquier momento. La comunicación podrá producirse en el momento y en la forma que se considere adecuado para asegurar el buen fin de la investigación, es decir, evitar que se pueda facilitar la ocultación, destrucción o alteración de las pruebas.

Por lo tanto, la norma por un lado indica que hay que facilitar el acceso al expediente y por otro lado indica que lo que hay que hacer es informar sobre las acciones u omisiones que se atribuyen al investigado. Es decir, en todo caso, el denunciado será informado del proceso de investigación que se está llevando a cabo para que pueda ejercer su derecho de defensa y alegar todo aquello que le permita acreditar su no implicación en los hechos pero no se indica de forma indubitada que deberá tener acceso completo o parcial al expediente.

Desde mi punto de vista, las organizaciones podrán (i) informar de las acciones u omisiones atribuidas de forma sucinta, (ii) podrán dar un acceso parcial al expediente o, (iii) de forma voluntaria podrán basarse en las previsiones legales diseñadas para la Autoridad Independiente de Protección del Informante, -en lo sucesivo, A.A.I- y aplicarlas

por analogía, al final de cuentas, la A.A.I puede investigar y podrá valorar la aplicación por analogía de las organizaciones privadas. En cualquier caso, las organizaciones deberán garantizar el derecho a la defensa y presunción de inocencia del investigado siendo potestativo por parte de la organización que diseñe el canal dar acceso total o parcial al expediente. Sería conveniente que el “canal de denuncias” o sistema interno de información pudiera facilitar esta funcionalidad para el caso que así lo determinara la organización de turno.

Como se indica dar acceso del expediente completo -con las salvaguardas al informante- es potestativa de la regulación de cada organización por los motivos indicados aunque deberá valorarse y se recomienda documentar la justificación para dar o no acceso total o completo al expediente.

Por lo tanto, las organizaciones deberán evaluar cómo garantizar el derecho a la defensa y a la presunción de inocencia del investigado. Pueden basarse en lo regulado para las A.A.I y aplicarlo por analogía para facilitar el acceso al expediente tal y como lo regula el artículo 19.2.

Instrucción: Se garantizará que la persona afectada por la información tenga noticia de la misma, así como de los hechos relatados de manera sucinta. No obstante, 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. Siempre con la salvaguarda de no comunicar a los sujetos afectados la identidad del informante ni se dará acceso a la comunicación. Durante la instrucción se dará noticia de la comunicación con sucinta relación de hechos al investigado. 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.

El artículo 19.3 regula a fin de garantizar el derecho 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.

Hay que tener en cuenta que el modelo de cumplimiento deberá velar durante el transcurso de las investigaciones internas, por el respeto de los derechos básicos de todo proceso justo, entre los

que se engloban el derecho a ser informado con claridad de los hechos que se le atribuyen, revisión de las distintas pruebas que existan en su contra y acceso al expediente de la investigación – sin desvelar el contenido protegido por la normativa de protección de datos–, derecho a hacer las alegaciones y presentar las pruebas que considere oportunas, contar con la presencia de un abogado, respeto a la presunción de inocencia, la posibilidad de recurrir la decisión que se adopte.

En esta línea el artículo 22 de la Directiva (UE) 2019/1937.

Está claro que la normativa tiende a facilitar el acceso al expediente en los términos establecidos.

Para finalizar y en otro orden de cuestiones a modo de sugerencia, considero interesante que pudiera darse la opción de habilitar en la herramienta que se utilizara “canal de denuncia” una opción para informar al informante sobre el estado de la tramitación de la comunicación o “denuncia” que ha realizado. En ocasiones los informantes ante la ausencia de comunicaciones por parte del órgano encargado de tramitar el expediente puede ocasionar determinadas actitudes que conlleven a solicitar medidas de apoyo externas y de esta forma podría ayudar a mitigar esta reacción.

METADATOS

Lo que la ley indica es que (Artículo 32. Tratamiento de datos personales en el Sistema interno de información.)

3. Los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.

Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda.

constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

4. En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32

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

En el entendido que los metadatos constituyen información sobre los datos y como consecuencia de que podrían constituir información sobre la denuncia, y en cumplimiento de las directrices de protección de datos en esta ley y en la propia Ley 3/2018 de Protección de Datos Personales y garantía de derechos digitales, nuestra interpretación es que se debe eliminar toda información que pueda afectar a esa denuncia, salvo que se mantenga anonimizada, incluidos los metadatos si con los mismos se consiguiera la obtención de información sobre la denuncia, sus características, sujetos vinculados, u otra información propia de la comunicación.

DERECHO A NO AUTOINCUCLPARSE

El pasado 12 de enero participamos como panelistas en la mesa redonda “La Directiva UE de protección al informante y su implementación práctica en España” con motivo de la convocatoria del II Foro Técnico Internacional de Compliance organizado por Aranzadi. Entre varias cuestiones, de máximo interés y relevancia, nos gustaría compartir con vosotros varias reflexiones sobre la materia.

La primera reflexión, se relaciona con la obligación de informar de los delitos al Ministerio Fiscal que prevé la normativa y el derecho

de la persona jurídica a no inculparse y a su legítima defensa. Si en el curso de una investigación interna que la ley reconoce, los hechos pudieran ser indiciariamente constitutivos de delito, la persona jurídica se verá obligada a calificar el delito con las dificultades prácticas y la carencia de garantías que esta situación provoca. La previsión normativa nos invita a valorar si la información recibida en el sistema interno de información se configura como una mera información que podrá ser objeto de investigación interna o también como prueba indiciaria

teniendo en cuenta todos los aspectos que implica. Todo ello teniendo en cuenta que la persona jurídica deberá contar con las mismas garantías de defensa que las personas físicas, entre otras, a no ser objeto de indefensión, el derecho a la tutela judicial efectiva, a la presunción de inocencia y el derecho a no autoincriminarse. Por lo tanto, el cumplimiento de esta obligación impuesto por la Ley 2/2023, tiene un difícil encaje en la configuración del resto de nuestro ordenamiento jurídico.

DELITOS COMPRENDIDOS EN EL ALCANCE OBJETIVO DE LA NORMA

En cuanto a los delitos que están dentro del alcance objetivo de la normativa referida, se llega a la conclusión que tienen cabida todos los delitos del Código Penal español. En este sentido, nos preguntamos si resulta proporcionado y adecuado o, si por el contrario no hubiera sido deseable que se incluyeran los delitos de los que la persona jurídica fuera responsable y, a voluntad de cada organización pudiera ser extensible a aquellos delitos sobre los que aunque no sean responsables las personas jurídicas puedan ser afectados por razón de su actividad.

SUJETOS PROTEGIDOS POR LA NORMATIVA

Sobre los sujetos a los que la norma protege por comunicar informaciones se considera necesario realizar varias reflexiones de la norma. Para que la protección se active deben darse varias condiciones como que se tengan motivos razonables para pensar que la información referida es veraz pero esto implica que sea información contrastada, por lo tanto las informaciones que no se consideren veraces y, por lo tanto, no admitidas no serán objeto de protección. Tampoco lo

serán aquellas informaciones que hayan sido inadmitidas con carácter previo, aquellas que no contengan información nueva y significativa sobre infracciones de una comunicación anterior sobre la que han concluido los procedimientos, cuando sean inverosímiles, cuando la información no sea constitutiva de infracción del ordenamiento jurídico, cuando carezca de fundamento o existan indicios racionales de haberse obtenido mediante la comisión de un delito.

Estos supuestos aplicados a la práctica pueden dar lugar a una suerte de casuísticas en las que los informantes quedarían desprotegidos en la creencia que sí lo están.

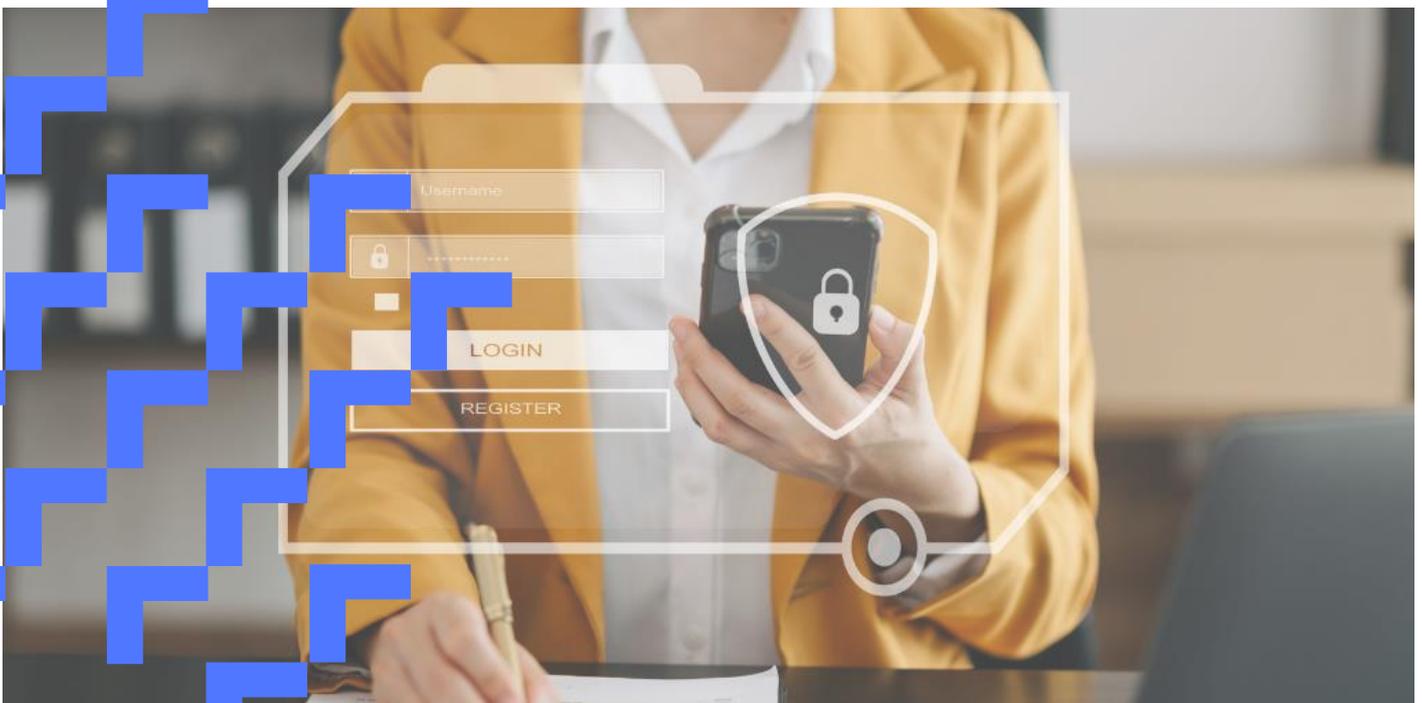
Deberemos atender a la evolución sobre la puesta en práctica de las disposiciones contenidas en la normativa y estar atentos a las circulares y recomendaciones que pueda publicar la Autoridad Independiente del Informante cuando se cree.

LA RELACIÓN SOBRE EL TRATAMIENTO CONFIDENCIAL DE LAS INFORMACIONES CON EL DERECHO DEL INVESTIGADO A CONOCER LOS HECHOS QUE SE LE ATRIBUYEN PARA PODER DEFENDERSE

La segunda reflexión, se refiere a la relación sobre el tratamiento confidencial de las informaciones con el derecho del investigado a conocer los hechos que se le atribuyen para poder defenderse. En este sentido, cabe recordar que el concepto de confidencialidad se refiere a la garantía que los datos no saldrán de la esfera de confianza en relación a la finalidad para la que serán tratados y por el que han sido reconocidos. Partiendo de esta base, el texto normativo determina que la configuración de los sistemas internos deberá contemplar el derecho del

que la configuración de los sistemas internos deberá contemplar el derecho del investigado a ser informado sobre los hechos sobre los que se le investiga. Por lo tanto, cuando se le informe al investigado, la identidad de informante, así como el resto de partes involucradas no deberán ser desveladas, pero surge el interrogante si por la propia naturaleza de la investigación o del contenido de la información, la identidad del informante pueda comprometerse. Hay que tener en cuenta que para los canales internos, la normativa no establece un procedimiento de gestión de la investigación y, por ende, tampoco lo relacionado con la comunicación, ni con la forma

en la que ésta deba realizarse, por lo tanto, serán las organizaciones las encargadas de diseñar e implementar diferentes soluciones. Como cuestión adicional, hay que tener en cuenta que la posición de la organización en una investigación interna puede tener diferentes estrategias, como la investigación con ulteriores intenciones de iniciar un procedimiento ante los Jueces y Tribunales competentes y por cumplimiento a la normativa aplicable, ésta se ve obligada a informar al investigado antes de iniciar la acción legal. Además de lo anterior deberá tenerse en cuenta las previsiones normativas de protección de datos personales.



¿La norma exige la obligatoriedad de implementar un canal de informaciones que implique la recepción de informaciones verbales?



En el ámbito privado existen condicionamientos para su buen funcionamiento, entre otros, la entidad y sus directivos se sientan verdaderamente comprometidos con la implantación de una cultura de la legalidad. Las vías de las que dispone el alertador para denunciar la existencia de irregularidades son tres:



La denuncia interna en los órganos competentes designados por las organizaciones en el sector público y privado.



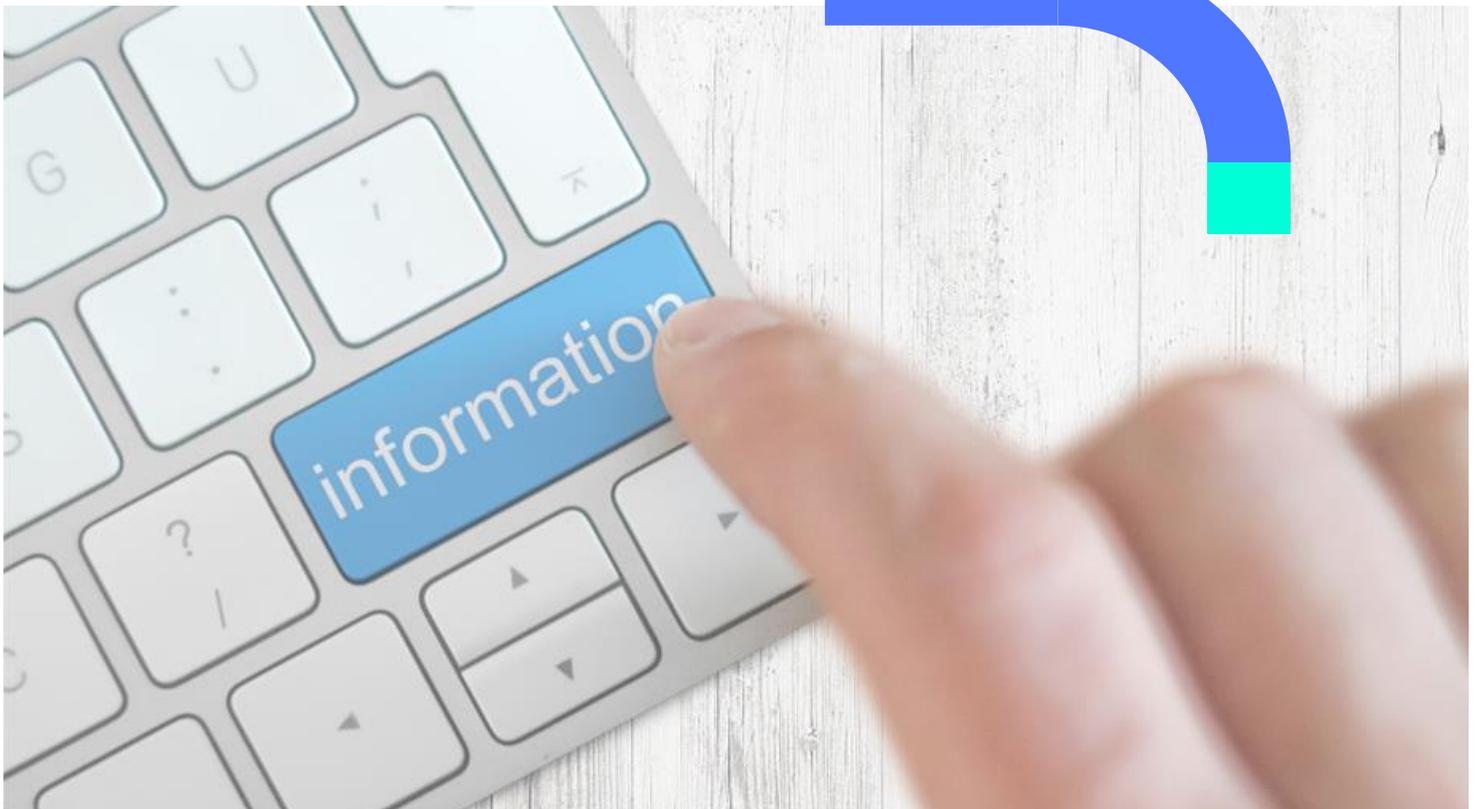
La denuncia externa ante las autoridades competentes designadas por los Estados miembros.



La revelación pública, como por ejemplo a través de los medios de comunicación.

Para cumplir con la norma deberá valorarse que:

- El canal de denuncias se ha implementado.
- Reúna las características como determinar quiénes pueden acceder, garantizar protección del informante, ser accesible, que el procedimiento para informar un riesgo del modelo no sea farragoso.
- Que se dé curso a la denuncia y se analice.
- Decretar la apertura de una investigación interna en el caso que se aprecie que la información es fundada.



La norma ISO 37002:2021 en el mismo sentido al comentar que lo esencial es garantizar la confidencialidad y anonimato.



Contextualizado lo anterior nos referimos a la configuración de los sistemas internos de información, para ello resulta conveniente referirnos al artículo 5.2 de la Ley del Informante que entre otros aspectos destacamos los siguientes por dar respuesta a la consulta planteada:

01

Estar diseñados, establecidos y gestionados de 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, la protección de datos, impidiendo el acceso de personal no autorizado.

02

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

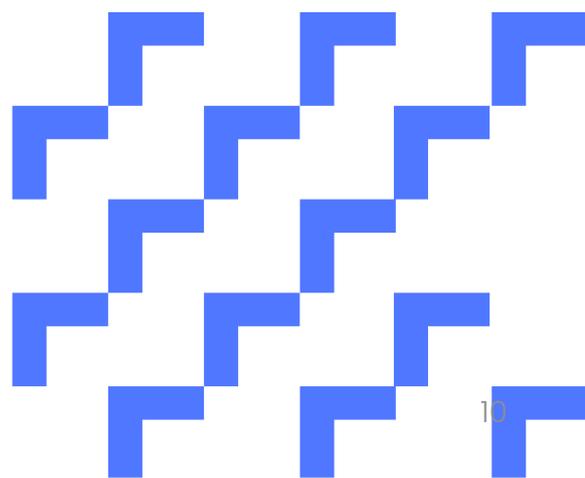
En cuanto al formato de los canales internos de información nos referimos al artículo 7.2 de la Ley del Informante que dispone que los canales internos deberán permitir realizar comunicaciones por escrito o verbalmente o, de las dos formas.

Por lo tanto, la información se podrá realizar 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 del sistema de mensajería de voz. Además, a solicitud del informante podrá presentarse mediante una reunión presencial dentro del plazo máximo de siete días.

La cuestión que deberá tener en previsión el responsable es que las comunicaciones verbales que podrán ser vía telefónica u otro sistema de mensajería de voz -lo deja a elección-, incluyendo las realizadas a través de reunión presencial, telefónicamente o mediante sistema de mensajería de voz, deberán estar documentadas de alguna de las formas (i) grabación de la conversación o, (ii) transcripción completa y exacta de la conversación.

En el mismo sentido la regulación para la recepción de informaciones del canal externo que pueden arrojar interpretación por analogía, del artículo 17 de la Ley del Informante "(...) La información se podrá realizar por escrito, a través de correo postal o a través de cualquier medio electrónico habilitado al efecto dirigido al canal externo de informaciones de la Autoridad Independiente de Protección del Informante, A.A.I., o verbalmente, por vía telefónica o a través de sistema de mensajería de voz (...)". En este sentido podemos verificar que vuelve a dejarlo a elección de la Autoridad Independiente de Protección al Informante la configuración del canal.

Como conclusión, tal y como dicta la norma, el canal puede estar configurado para recibir comunicaciones escritas o verbales o de ambas formas, no siendo obligatorio establecer ambas opciones, más bien parece dejarlo a voluntad del órgano de gobierno de cada organización pudiendo optar por un diseño que admita comunicaciones (i) verbales, (ii) escritas, (iii) verbales y escritas. A lo que obliga el canal es que las organizaciones establezcan la posibilidad de comunicar informaciones (i) con reserva de identidad y, (ii) anónimas, cuestión diferente es la configuración sobre si se admite la forma verbal o escrita o ambas, que tal y como se deduce es opcional por parte de las organizaciones.





PLAZOS DE CONSERVACIÓN

En relación a los plazos que puede durar la investigación, con carácter ordinario son tres meses, pero ante casos de especial complejidad para los canales internos puede prorrogarse por tres meses adicionales.

Para el caso que sirva de ayuda, en cuanto a los plazos de conservación de la información la Ley de Informantes determina lo siguiente:

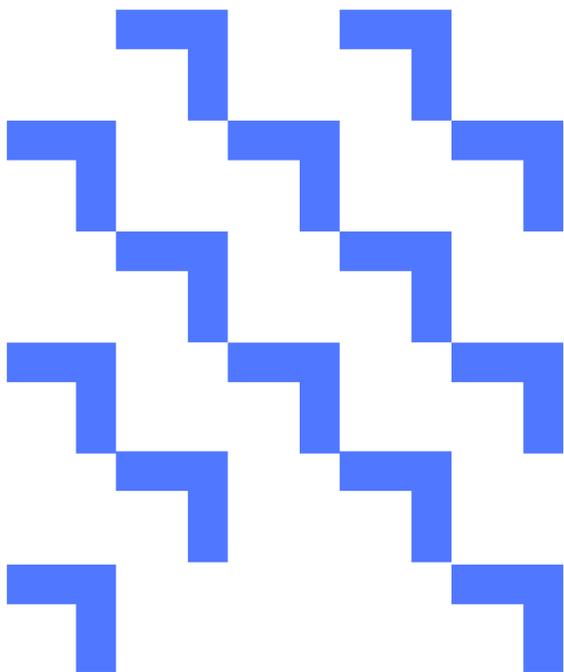
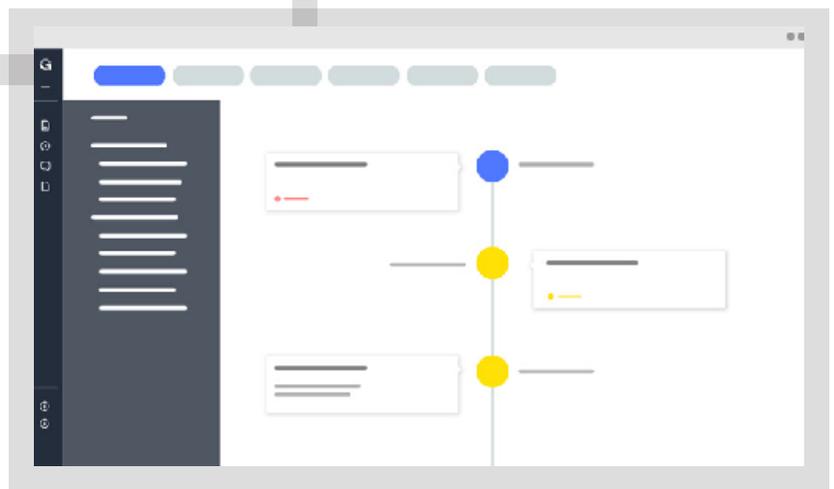
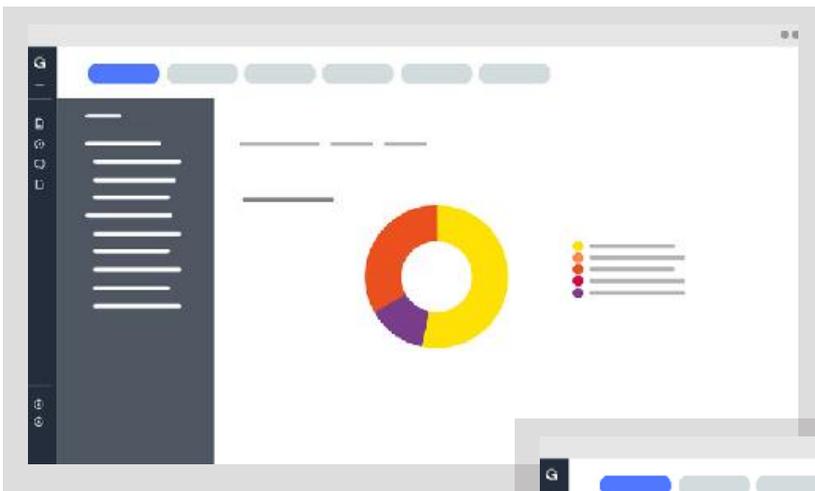
- Aquellas informaciones que se reciben pero se decide la no admisión -fuera del ámbito de aplicación de la norma, o fuera de las infracciones a las que el canal se hubiera podido hacer extensible- deberán de ser suprimidas de forma inmediata.
- Las comunicaciones a las que no se hubiera dado curso, solo podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo del 32 de la LOPDGDD.
- En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, se procederá a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema.
- Aquellas informaciones que se reciben pero se decide la no admisión -fuera del ámbito de aplicación de la norma, o fuera de las infracciones a las que el canal se hubiera podido hacer extensible- deberán de ser suprimidas de forma inmediata.
- Las comunicaciones a las que no se hubiera dado curso, solo podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo del 32 de la LOPDGDD.
- En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, se procederá a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema.
- Si la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que la falta de veracidad pueda constituir un ilícito penal, en cuyo caso se custodiará la información durante el trámite del procedimiento judicial.
- Si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de los mismos. En este punto, la Ley también establece una base de legitimación para el tratamiento de categorías especiales de datos, ergo, pueden ser tratados.

De forma complementaria a estos plazos hay que tener en cuenta los libros-registros, que son repositorios en el que se deja constancia de todas las comunicaciones recibidas, su tramitación, respuestas, etcétera. En este caso los datos personales de las informaciones recibidas y a las investigaciones internas se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con la Ley, teniendo en cuenta lo previsto en el párrafo

anterior y, en ningún caso podrán conservarse por un período superior a diez años.

En cuanto al comienzo del expediente también entiendo que comprende todas las fases del desarrollo de una investigación interna -desde la fase preliminar que incluye la recogida y valoración de admisión de la información recibida hasta la conclusión de la investigación-. La Ley de Informantes no regula el procedimiento de investigación

para los canales internos pero sí lo hace para los canales externos diferenciando las etapas que se desglosan en (i) trámite de admisión, donde se inadmite o inadmite la comunicación, (ii) instrucción, (iii) terminación de actuaciones.



Acerca de los autores



María del Águila Bigorra

Es licenciada en Derecho en la Universidad de Alcalá de Henares y especializada en derecho de las nuevas tecnologías, protección de datos y comercio electrónico. Profesionalmente ejerce en GlobalSuite Solutions como consultora senior de privacidad experta en el Reglamento General de Protección de Datos Personales, apoyando en su implantación a empresas de diferentes países y sectores: automoción, logística, seguros, bancario... Adicionalmente, pertenece al equipo del Área de Compliance de la organización dando apoyo legal a todas las áreas que la integran.

GlobalSuite Solutions

En GlobalSuite Solutions nos dedicamos a aportar e implementar soluciones en materia de Riesgos, Seguridad, Continuidad, Cumplimiento legal, Privacidad y Auditoría, entre otros.

Nuestra solución [GlobalSuite® Canal de Denuncias](#) cuenta con una serie de soluciones preconfiguradas para marcos a nivel global, regional y local. Podrás empezar a trabajar desde el primer día, sin tener que invertir tiempo cargando catálogos de cumplimientos, catálogos de riesgos y controles, ni metodologías. Todo está preparado para optimizar los tiempos y permitir centrarte en lo más importante: tus objetivos y tus procesos.

Contamos con más de 15 años de experiencia y más de 2.000 clientes en empresas de múltiples sectores como el financiero, asegurador, industrial, transporte, telecomunicaciones, energético, público, etc.

GlobalSuite® es la solución GRC para optimizar los procesos de riesgos, seguridad, continuidad, auditoría, privacidad y compliance en tu negocio.

Para más información o una demo gratuita de cómo su organización puede automatizar sus procesos de GRC, agende una reunión con [nuestro equipo](#) o visite <https://www.globalsuitesolutions.com/es/>