



RavenPack

Canal de Denuncias

Sistema Interno de Información

Tabla de contenido

Canal Interno de Información	3
Introducción	3
Proposito	4
Principios	4
¿Que puede ser reportado? - Ambito material de aplicación	5
¿Quien puede reportar? - Ambito personal de aplicación	5
Contenido de las comunicaciones / denuncias	6
Responsable del Sistema Interno de Información	7
Protección del informante y de las personas afectadas	7
Proteccion de Datos Personales	9
Procedimiento	10
Preguntas	10

Política del Canal de Denuncias

Canal Interno de Información

Introducción

En cumplimiento de lo establecido en la Ley española 2/2023, de 20 de febrero, que regula la protección de las personas que informan sobre infracciones normativas y combate la corrupción, RavenPack International SLU ("RavenPack") ha implementado un Sistema de Información Interno, en adelante "SII".

El SII funciona como un canal para aquellas personas que, en un contexto laboral o profesional, hayan obtenido información sobre acciones u omisiones que puedan constituir infracciones a la ley de la Unión Europea o delitos administrativos o penales graves o muy graves en el ámbito de RavenPack, para informar sobre ellas con todas las garantías de confidencialidad y protección.

La ley contempla la existencia de dos tipos de sistemas de información a los que el público puede recurrir para informar con garantías de confidencialidad y anonimato:

- Interno: Este sirve como el canal preferido para informar sobre acciones u omisiones cubiertas por la ley, siempre que la infracción pueda abordarse de manera efectiva. Es preferible que la información sobre prácticas irregulares sea conocida primero por RavenPack misma para corregirlas o reparar los daños lo antes posible.
- Externo: Dirigido a proporcionar al público una comunicación a una autoridad pública especializada, para estos fines, la Autoridad Independiente de Protección del Informante o Autoridad Independiente para la Protección de Denunciantes ("A.A.I."), o las autoridades regionales competentes. Este canal puede inspirar más confianza en las personas, disipando su temor a represalias en su entorno. En nuestro caso, como empresa con sede en la región de Andalucía, España, la A.A.I. correspondiente es la Oficina Andaluza Antifraude, disponible en <https://antifraudeandalucia.sedelectronica.es/>

Sin embargo, es un derecho del informante evaluar qué canal seguir, interno o externo, en función de las circunstancias y los riesgos de represalias que se consideren.

Proposito

El Sistema de Información Interno establecido por RavenPack tiene un doble propósito:

- Protección de Individuos: Su objetivo es proteger a las personas en un contexto laboral o profesional que detecten y denuncien infracciones normativas y actos de corrupción (denominadas "Informantes" o "Denunciantes"). Además, se extiende la protección a las personas que son objeto de los hechos denunciados.
- Fortalecimiento de la Cultura de Información o Comunicación: El sistema está diseñado para fortalecer la cultura de información o comunicación dentro de la organización. Esto sirve como un mecanismo para prevenir y detectar amenazas al interés público.

Principios

Con el objetivo de garantizar la efectividad del sistema, RavenPack se asegurará de que cumpla con todos los requisitos establecidos en la Ley 2/2023, que regula la protección de las personas que informan sobre infracciones normativas y combate la corrupción, en particular:

- Accesibilidad: El SII debe permitir la comunicación, ya sea por escrito, verbalmente, o ambas, de información sobre infracciones normativas y la lucha contra la corrupción a todas las personas dentro de su ámbito de aplicación.
- Independencia: El SII será gestionado por un Oficial de Denuncias con completa independencia y autonomía respecto al resto de sus órganos.
- Confidencialidad: Se garantiza la confidencialidad de la identidad del Informante y de cualquier persona mencionada en la comunicación, así como de las acciones realizadas en su gestión y procesamiento. El canal de información interno incluso permitirá la presentación y posterior procesamiento de comunicaciones anónimas.
- Protección de Datos Personales.
- Secreto de las Comunicaciones.
- Seguridad y Protección de los Informantes y Personas Afectadas.
- Presunción de Inocencia y Respeto a la Dignidad de las Personas Afectadas.

¿Que puede ser reportado? - Ambito material de aplicación

El SII debe permitir la recepción de comunicaciones relacionadas con eventos que podrían constituir, dentro del ámbito de competencias de RavenPack:

- Acciones u omisiones que puedan constituir violaciones de la legislación de la Unión Europea, siempre que:
 - - Se encuentren dentro del ámbito de aplicación de los actos de la Unión enumerados en el Anexo de la Directiva (UE) 2019/1937, independientemente de la clasificación realizada por el sistema legal nacional. La directiva establece reglas mínimas comunes para la protección de las personas que informan sobre las siguientes violaciones de la legislación de la Unión: Violaciones que entren dentro del ámbito de los actos de la Unión enumerados en el anexo relacionados con las siguientes áreas: i) contratación pública, ii) servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo, iii) seguridad y conformidad de productos, iv) seguridad en el transporte, v) protección del medio ambiente, vi) protección contra la radiación y seguridad nuclear, vii) seguridad alimentaria y de piensos, salud animal y bienestar animal, viii) salud pública, ix) protección del consumidor, x) privacidad y protección de datos personales, y seguridad de redes y sistemas de información.
 - - Afecten a los intereses financieros de la Unión Europea, según lo contemplado en el Artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE).
 - - Impacten en el mercado interno, según lo contemplado en el Artículo 26, párrafo 2 del TFUE, incluyendo violaciones de las normas de la Unión sobre competencia y ayudas estatales, así como violaciones relacionadas con el mercado interno en lo que respecta a actos que infringen las normas fiscales corporativas o prácticas destinadas a obtener una ventaja fiscal que distorsiona el propósito o la intención de la legislación aplicable a impuestos corporativos.
- Acciones u omisiones que puedan constituir delitos graves o muy graves, en cualquier caso, esto incluye todos los delitos graves o muy graves, tanto criminales como administrativos, que impliquen pérdida económica para la Agencia Tributaria y la Seguridad Social españolas.

¿Quien puede reportar? - Ambito personal de aplicación

El SII permite la denuncia de posibles violaciones por parte de individuos que trabajan tanto en el sector privado como en el público, y que han obtenido información sobre infracciones en un contexto laboral o profesional. Esto abarca lo siguiente:

- Todas las personas que tengan el estatus público de empleados de RavenPack.
- Todos los profesionales autónomos, proveedores, contratistas, subcontratistas, o cualquier otro tercero con quienes RavenPack tenga o haya tenido previamente alguna

relación comercial o profesional. Esto incluye a todas las personas que trabajen para ellos o bajo la supervisión o dirección de contratistas, subcontratistas y proveedores de RavenPack.

- Cualquier persona que haya tenido una relación laboral o estatutaria terminada con RavenPack, voluntarios, becarios, practicantes, independientemente de si reciben remuneración o no, e incluso personas que participan en procesos de selección de personal, siempre que la información sobre la infracción se haya obtenido durante el proceso de selección o negociación precontractual.

Las medidas de protección al denunciante también se aplicarán, si corresponde, específicamente a los representantes legales de los trabajadores en el ejercicio de sus funciones de asesoramiento y apoyo al denunciante.

La persona que proporcione información debe tener una creencia razonable en la exactitud de la información comunicada y no debe realizar comunicaciones de mala fe o abuso de derecho. En este último caso, pueden incurrir en responsabilidad civil, penal y administrativa.

Contenido de las comunicaciones / denuncias

La comunicación o denuncias presentada debe incluir el máximo número de detalles conocidos necesarios para la identificación de las personas a las que se refiere la información, así como los comportamientos contrarios a las disposiciones legales que se les atribuyen. En particular, se deben proporcionar los siguientes datos:

- Nombre completo, número de DNI (si se conoce), lugar de trabajo, área funcional, cargo, ubicación donde desempeñan sus funciones y cualquier otro dato disponible que permita la identificación clara y inequívoca de la persona sobre la cual se está informando.
- Descripción detallada de las acciones y comportamientos realizados que puedan constituir cualquier tipo de violación y sobre los cuales se pretende informar. Se debe proporcionar documentación disponible para respaldar estos hechos.
- Si corresponde, indicación de la relación laboral o profesional que vincula al informante con RavenPack, con el fin de aplicar las medidas de protección.
- Cualquier otro hecho que se considere apropiado o relevante.

Al realizar la comunicación, el informante puede especificar una dirección, correo electrónico o ubicación segura para recibir notificaciones. El informante también puede renunciar expresamente a recibir cualquier comunicación sobre las acciones tomadas como resultado de la información proporcionada.

Responsable del Sistema Interno de Información

El CEO de RavenPack es responsable de implementar el Sistema de Información Interno (IIS) y del tratamiento de datos personales. Además, tienen la autoridad para designar, destituir o reemplazar a la persona responsable del IIS. La persona designada como Responsable del Sistema Interno de Información por la dirección de RavenPack es el Asesor Jurídico de RavenPack.

El Responsable del Sistema Interno de Información tiene la tarea de gestionar diligentemente el IIS y de manejar adecuadamente las comunicaciones recibidas.

El Responsable del Sistema Interno de Información *"debe desempeñar sus funciones de manera independiente y autónoma respecto al resto de los órganos o entidades de la entidad, no puede recibir ningún tipo de instrucción en su ejercicio y debe contar con todos los recursos personales y materiales para llevarlas a cabo"*.

Protección del informante y de las personas afectadas

Las personas que informen sobre infracciones tendrán derecho a protección.

Preservación de la identidad del informante y las personas afectadas:

Preservación la identidad de la persona denunciante cuando así esta lo solicite, excepto en aquellas comunicaciones que puedan hacerse a la autoridad judicial, la Fiscalía o la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.

Condiciones para la Protección:

Las personas que informen o revelen infracciones dentro del ámbito material de aplicación tienen derecho a protección siempre que existan las siguientes circunstancias:

- Tengan motivos razonables para creer que la información es verdadera en el momento de la comunicación o revelación, incluso si no se proporcionan pruebas concluyentes, y que la información esté dentro del ámbito de la ley.
- La comunicación o revelación se haya hecho de acuerdo con los requisitos estipulados por la ley.

La protección establecida en esta ley se excluye explícitamente para las personas que informan o revelan:

- Información contenida en comunicaciones que hayan sido rechazadas por cualquier canal interno de información o por la A.A.I.
- Información relacionada con reclamaciones sobre conflictos interpersonales o que solo afecten al informante y a las personas mencionadas en la comunicación o revelación.

- Información que ya esté completamente disponible al público o que constituya meros rumores.
- Información relacionada con acciones u omisiones no cubiertas por el Artículo 2 de la Ley 2/2023.
- Personas que hayan informado o revelado información de manera anónima sobre acciones u omisiones de forma pública, pero que luego hayan sido identificadas y cumplan con las condiciones especificadas para tener derecho a la protección.

En cuanto a las comunicaciones falsas, la Ley 2/2023 establece que comunicar conscientemente o revelar públicamente información falsa constituye una infracción muy grave.

Prohibición de Represalias y Medidas de Protección contra los Denunciantes:

El sistema establece el principio de protección del denunciante, prohibiendo expresamente cualquier acto de represalia, amenaza de represalia o intento de represalia contra el denunciante.

Se entiende que las represalias incluyen cualquier acto u omisión prohibido por la ley, o que, directa o indirectamente, resulte en un trato desfavorable colocando a aquellos que las sufren en una desventaja particular en comparación con otros en el contexto laboral o profesional, únicamente debido a su condición de denunciantes o por hacer una divulgación pública.

Como se especifica en el Artículo 36.3 de la Ley 2/2023, "a título ilustrativo", las represalias incluyen actos como:

- Suspensión del contrato de trabajo, despido o terminación de la relación laboral o estatutaria, incluyendo la no renovación o terminación anticipada de un contrato de trabajo temporal una vez superado el período de prueba, o la 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 laborales y la no conversión de un contrato de trabajo temporal en uno permanente, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un empleo permanente; a menos que estas medidas se realicen dentro del ejercicio regular del poder de dirección según la ley laboral o de servicio civil, debido a circunstancias, hechos o infracciones probadas, y no relacionadas con la presentación de la comunicación.
- Perjuicios, incluyendo pérdidas reputacionales o económicas, coerción, intimidación, acoso u ostracismo.
- Evaluaciones o referencias negativas sobre el desempeño laboral o profesional.
- Inclusión en listas negras o difusión de información en un sector específico que dificulte o impida el acceso al empleo o la contratación de obras o servicios.
- Denegación o anulación de una licencia o permiso.
- Denegación de formación.
- Discriminación o trato desfavorable o injusto.

Medidas para la Protección de Personas Afectadas:

Las personas afectadas por la comunicación, durante el proceso del caso, tendrán derecho a:

- La presunción de inocencia.
- La defensa.
- Acceder al expediente del caso en los términos regulados en la Ley 2/2023.
- La misma protección establecida para los denunciantes, preservando su identidad y garantizando la confidencialidad de los hechos y datos del procedimiento. Se exceptúa en el caso de comunicaciones que puedan hacerse a la autoridad judicial, la Fiscalía o la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.
- La exención o mitigación de la sanción que les pueda corresponder si se cumplen los requisitos siguientes:
 - Haber cesado en la comisión de la infracción en el momento de presentar la comunicación o revelación y haber identificado, en su caso, al resto de las personas que han participado o favorecido.
 - Haber cooperado plena, continua y diligentemente a lo largo de todo el proceso de investigación.
 - Haber proporcionado información veraz y relevante, pruebas o datos significativos para fundamentar los hechos investigados, sin haber procedido a su destrucción o ocultamiento, ni haber revelado su contenido a terceros, directa o indirectamente.
 - Haber procedido a reparar el daño causado por el cual son responsables.

Protección de Datos Personales

El tratamiento de datos personales resultante de la aplicación de la Ley 2/2023 estará regido por las disposiciones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, y la Ley Orgánica 7/2021, de protección de datos personales tratados con fines de prevención, detección, investigación y sanción de infracciones penales y ejecución de sanciones penales.

El SII debe prevenir el acceso no autorizado, preservar la identidad y garantizar la confidencialidad de los datos relacionados con las personas afectadas y cualquier tercero mencionado en la información proporcionada, especialmente la identidad del denunciante si este ha sido identificado.

La identidad del denunciante solo podrá ser revelada a la autoridad judicial, la Fiscalía o la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora. En tales casos, estarán sujetos a las salvaguardias establecidas en las regulaciones aplicables.

Si la información recibida contiene datos personales sujetos a protección especial, se llevará a cabo su eliminación inmediata a menos que el tratamiento sea necesario por razones de interés público esencial. En cualquier caso, no se recopilarán datos personales que no sean

evidentemente relevantes para el procesamiento de información específica, o si se recopilan accidentalmente, se eliminarán de inmediato.

Las comunicaciones que no hayan sido procesadas se retendrán solo en forma anonimizada, y no se aplicará la obligación de bloqueo.

Procedimiento

Para obtener más información sobre el procedimiento del SII, por favor consulta nuestro Procedimiento del Canal de Denuncias.

Preguntas

Si tienes alguna pregunta o consulta sobre esta política, por favor contáctanos en whistle@ravenpack.com.