guía del INFORMANTE

contenido
DE LA GUÍA

– INTRODUCCIÓN –

Esta guía está dirigida principalmente a aquellas personas qe formulen una denuncia o Comunicación en nuestro Canal del Sistema de Información (en adelante, SII) pudiendo encontrar en el mismo los diversos aspectos e implicaciones de nuestro Canal explicados de manera sencilla y comprensible.

Principalmente le explicamos qué vamos a hacer con su información, qué implicaciones tiene la consideración de informante y cómo vamos a protegerlo. Asimismo, también encontrará información acerca de las la Autoridad Independiente de Protección de la Persona Informante (en adelante A.A.I.), cómo le pueden proteger y qué medidas tiene a su disposición, qué son los canales de denuncia externos y, por último, qué consecuencias le puede comportar habernos aportado información falsa, obtenida delictivamente o manipulada.

– ¿QUÉ VAS A ENCONTRAR EN ESTA GUÍA? –

Esta guía tiene como objetivo informar a cualquier persona interesada en presentar una denuncia o comunicación al Sistema Interno de Reportes de Incidentes (RSI) sobre los siguientes aspectos relevantes:

1. Los canales internos que RSI ofrece y cómo operan.

2. Las medidas de protección que RSI implementa para las personas que informan o denuncian posibles infracciones.

3- Los canales externos disponibles para los informantes.

Además, junto a esta guía, encontrará los siguientes documentos:

- La Política del Sistema Interno de Información aprobada por RSI.

- La Política de Privacidad aprobada por RSI para la gestión adecuada de la información y los datos personales canalizados a través de los canales internos y el Sistema Interno de Información.

– HECHOS E INFRACCIONES SUSCEPTIBLES DE COMUNICACIÓN –

¿QUÉ HECHOS PUEDO COMUNICAR?

A través de los diversos Canales habilitados, usted podrá informar sobre cualquier hecho que crea que puede ser constitutivo de infracción.

La Comunicación que Usted quiera realizar tiene que estar relacionada con acciones u omisiones que en RSI tengamos capacidad para investigar, corregir y reparar, es decir, informaciones relacionadas con las conductas de los miembros de RSI o del resto de partes interesadas o socios de negocio que participan de las actividades, procesos y procedimientos de RSI.

Si su Comunicación no cumpliera este requisito, deberemos inadmitirla, aunque le indicaremos los canales internos y externos donde creemos que debe Usted dirigirse para formular su Comunicación.

¿EXISTE ALGUNA AYUDA PARA INDENTIFICAR LOS HECHOS O CONDUCTAS QUE PUEDO DENUNCIAR?

Para una mayor facilidad, RSI ha agrupado los hechos que pueden ser constitutivos de infracción en las siguientes conductas. Estas conductas podrán ser parte de acciones u omisiones, conforme a lo establecido en el artículo 2 de la Ley 2/2023:

- Cualquier acción u omisión que pueda constituir una infracción del Derecho de la Unión Europea que:

a. Entren en el 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,

b. O bien 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);

c. 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.

- Cualquier acción u omisión que pueda ser constitutiva de infracción penal, o administrativa grave o muy grave conforme a nuestro derecho interno y de forma particular, la infracción de la normativa reguladora de la prevención del blanqueo de capitales y financiación del terrorismo.
- Especialmente cualquier conducta tipificada en el Código Penal que pudieran dar lugar a la responsabilidad penal de las personas jurídicas recogidas en el SGCP de RSI.
- Cualquier irregularidad (error material o fraude) cometida en el proceso de emisión de Información Financiera y contable de RSI.
- Las violaciones del Código de Conducta de los Directivos y Empleados.
- Las violaciones de la Política de Conflictos de Interés de RSI.

En adelante, el conjunto de disposiciones legales y directrices internas mencionadas cuya infracción es susceptible de ser denunciada a través del SII o Canal de Denuncias y sus Canales de Comunicación, serán denominadas como “la Normativa”.

A continuación, incluimos información adicional para cada una de las conductas a seleccionar en el Canal:

1. Acoso:

- Acoso Sexual o por razón de sexo: Comportamiento irrespetuoso o conducta no deseada de carácter sexual que sea molesta y que genere un ambiente intimidatorio, ofensivo u hostil en el trabajo.

- Acoso laboral: Trato hostil o vejatorio de manera sistemática en el ámbito laboral que provoca un ambiente intimidatorio, ofensivo u hostil.

2. Ciberseguridad: Algunos de los riesgos o conductas delictivas contrarias a la Ciberseguridad son los siguientes:

- Acceso no autorizado o uso indebido de la información o los sistemas (p. ej., robo de información personal, planes de fusiones y adquisiciones o propiedad intelectual)

- Fraude financiero y robo (p. ej., desvío de pagos, extracción de fondos de cuentas de clientes, fraude de tarjetas de crédito, robo de identidad, etc.)

- Alteración de la actividad comercial (p. ej., sabotaje, extorsión, denegación de servicio).

3. Conflictos de interés: Situaciones en las que los intereses personales o financieros de un empleado - o los de sus familiares directos o cualquier persona con la que el empleado tenga una relación significativa - interfieran de alguna manera con su capacidad de servir a los mejores intereses de RSI, sus clientes, y/o sus partes interesadas.

4. Contabilidad y auditoría: Alteración o falsificación de la información financiera, inexactitudes en declaraciones financieras, falsedad intencionada en información, influencia indebida sobre los auditores, prácticas cuestionables en contabilidad, auditoría o controles financieros internos.

5. Contra la integridad moral: Son las acciones que causan daño psicológico o emocional a una persona. Estas acciones pueden incluir acoso moral o laboral, discriminación, difamación, violencia psicológica, ciber-acoso, o exclusión social, entre otras.

7. Contra los recursos naturales y medio ambiente: Entre otras acciones que atentan contra el medio ambiente nos encontramos con la contaminación y mala gestión de residuos, contaminación de gases del aire o contaminación del agua mediante vertidos de sustancias químicas, desechos industriales en cuerpos de agua no residuales.

8. Corrupción, Soborno y Cohecho: Un acto de corrupción puede surgir cuando un individuo abusa de su posición de poder o responsabilidad para su propio beneficio personal.

El soborno son actos que dan a alguien la ventaja financiera o de otro tipo para animar a esa persona a desempeñar sus funciones o

actividades de forma indebida o para recompensar a esa persona por haberlo ya realizado. Esto abarcaría el intento de influir en un responsable de la toma de decisiones mediante la concesión de algún tipo de beneficio adicional a dicho responsable, más allá de lo que puede ofrecerse legítimamente.

El cohecho se refiere al acto de ofrecer, dar, recibir o solicitar algo de valor a cambio de una ventaja personal o empresarial. El objeto de valor puede consistir en dinero, regalos, servicios u otros beneficios, y la ventaja buscada puede incluir la obtención o retención de negocios o la obtención de alguna otra ventaja indebida.

9. Daños informáticos: Acciones maliciosas que causan perjuicio o daño a sistemas informáticos, redes, equipos o datos electrónicos. Entre otros ejemplos nos encontramos con accesos no autorizados, distribución de malware, ataques de denegación de servicio (DDoS), intrusiones o hackeo, destrucción o alteración de datos, o phising entre otros

10. Defensa de la Competencia: Conductas que impidan, restrinjan o falseen la libre y efectiva competencia en detrimento del mercado, de los clientes de RSI y de todos aquellos con los que se mantengan relaciones comerciales y/o profesionales. Algunas de estas conductas son el intercambio de información sensible con competidores, los acuerdos sobre precios, el reparto de mercados, la manipulación de licitaciones o concursos.

11. Derechos y libertades de los extranjeros e integración social: Conductas contrarias a los derechos de libre circulación, reunión y manifestación, asociación, al trabajo y la Seguridad Social, de sindicación y de huelga se reconocen a los extranjeros que estén en situación legal de estancia o residencia.

12. Económicos: Todo incumplimiento relativo al funcionamiento de las sociedades de capital tal y como establece la Ley de Sociedades de Capital 1/2010 en España. Incluyéndose entre otros, las obligaciones relativas a la administración de la sociedad, cuentas anuales o participaciones.

14. Estafa: Acciones engañosas realizadas con el objetivo de obtener un beneficio económico o causar perjuicio a otra persona. Algunas acciones que pueden constituir estafa son fraude financiero, estafas en línea, estafas telefónicas, falsificación de documentos, estafas inmobiliarias, estafas de servicios, entre otras.

15. Facturación fraudulenta: Acciones relativas a la emisión o manipulación de facturas de manera engañosa o ilegal, con el objetivo de obtener beneficios económicos indebidos o evadir impuestos. Algunas situaciones en las que se puede cometer este delito son la facturación falsa, doble facturación, facturación inflada, facturación en negro, o facturación ficticia entre otros.

17. Faltas de respeto graves: Conductas que involucren faltas de respeto graves por parte de compañeros de trabajo o directivos en el entorno laboral.

18. Fraude:

- Fraude interno: Fraude intentado o perpetrado por una o varias partes internas contra la organización, es decir, un empleado o una filial de la organización, incluidos los casos en que un empleado actúa en colusión sin partes externas.

- Fraude externo: El tipo de fraude intentado o perpetrado por una parte (o partes) externa(s) contra la organización o los clientes con responsabilidad del banco. Puede haber casos en que una parte interna también esté involucrada en el fraude.

19. Igualdad de oportunidades y no discriminación: Conductas que no se encuentren alineadas con el principio básico de actuación en RSI relativo a proporcionar las mismas oportunidades en el acceso al trabajo y en la promoción profesional, asegurando en todo momento la ausencia de discriminación por razón de sexo u orientación sexual, raza, religión, discapacidad, origen, estado civil, edad o condición social.

20. Incumplimiento de comportamientos corporativos: Conducta no profesional por parte de compañeros de trabajo o directivos que no estén alineadas con los comportamientos corporativos o son contrarios al Código Ético de RSI.

21. Incumplimiento de normativa laboral: Todo incumplimiento de los reglamentos (legales o convencionales), políticas o procedimientos internos de RSI que implique el incumplimiento de una obligación laboral, así como de las categorizadas en el convenio colectivo vigente.

22. Incumplimiento de obligaciones contables:

Entre otras acciones susceptibles de suponer el incumplimiento de obligaciones contables nos encontramos con el registro y mantenimiento inadecuado de libros contables, falta de documentación adecuada, omisión de información relevante, o manipulación de información financiera entre otros.

23. Malversación: Entre las acciones susceptibles de malversación nos encontramos con el desvío de fondos, fraude contable, sobrefacturación o facturación ficticia, pago de sobornos, uso de recursos para gastos personales, entre otros.

24. Prevención de Blanqueo de Capitales y Financiación del Terrorismo y Sanciones: El blanqueo de capitales es: i) La conversión o la transferencia de activos a sabiendas de que dichos activos proceden de una actividad delictiva o de la participación en una actividad delictiva, con el fin de ocultar o encubrir el origen ilícito de los activos o de ayudar a las personas involucradas a evitar las consecuencias jurídicas de sus actos; ii) La ocultación o el encubrimiento de la naturaleza, el origen, la ubicación, la disponibilidad, el movimiento o la propiedad real de activos o derechos sobre activos a sabiendas de que dichos activos proceden de una actividad delictiva o de la participación en una actividad delictiva; iii) Adquirir, poseer o utilizar activos a sabiendas de que, en el momento de su recepción, dichos activos proceden de una actividad delictiva o de la participación en una actividad delictiva; iv) Participar en cualquiera de las actividades mencionadas anteriormente, asociarse para cometer este tipo de actividades, intentar realizarlas y prestar asistencia, instigación o asesoramiento a un tercero para que realice o facilite este tipo de actividad.

25. Prevención de riesgos laborales: Conductas contrarias a los derechos de los trabajadores, en particular, aquellas referentes a materia de seguridad y salud en el trabajo.

26. Propiedad Intelectual: Utilizar obras o prestaciones protegidas por derechos de autor, propiedad industrial o cualquier otro derecho reconocido en la LPI sin contar con la autorización expresa del titular, principalmente aquellos referidos contra los programas de ordenador y otras creaciones de RSI.

27. Protección de Datos, Seguridad de la Información y/o Confidencialidad de la información: La privacidad y la protección de la información implican abstenerse de difundir información a terceros, por ejemplo, información personal de clientes, de los empleados (sueldos, permisos, etc.), de seguridad/estratégica de RSI, así como la información relativa a las entidades con las que RSI mantiene relaciones comerciales. Estas obligaciones se mantienen incluso después de la terminación del empleo y se prohíbe el uso de la información confidencial para obtener beneficios económicos.

28. Publicidad: Conductas contrarias a la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y contra la Ley General para la Defensa de los Consumidores y Usuarios. Pueden serlos actos de publicidad engañosa, o las comunicaciones comerciales que no estén identificadas como tales, y que su envío por correo electrónico u otras vías de comunicación electrónica equivalente no hayan sido realizadas con el consentimiento del destinatario, entre otras.

29. Regalos e invitaciones: Cuando un profesional abusa de sus funciones en RSI ofreciendo, entregando, prometiendo, solicitando o aceptando cualquier tipo de regalo, beneficio/consideración o invitación para obtener una ventaja personal para él o un tercero, afectando a su imparcialidad.

30. Robo, uso indebido o abuso de bienes y recursos: El que, con ánimo de lucro, se apropia o abusa del uso de bienes o recursos ajenos sin la voluntad de su propietario, pudiendo causar un perjuicio patrimonial.

31. Secretos de empresa: Acciones que involucran la divulgación, robo o uso no autorizado de información confidencial y estratégica de la empresa. Algunas acciones que pueden poner en peligro los secretos de empresa son divulgación no autorizada, robo de información, espionaje industrial, uso indebido de información privilegiada, violación de acuerdos de confidencialidad, acceso no autorizado, o empleados desleales entre otros.

32. Seguridad: Todo incumplimiento relacionado con las instalaciones de protección contra incendios, así como del diseño, instalación y mantenimiento de los sistemas de protección **activa contra incendios. De la misma manera, todo incumplimiento relativo a la realización y la prestación por personas privadas, físicas o jurídicas, de actividades y de los servicios de seguridad privada suscrita para las instalaciones**

de confidencialidad, acceso no autorizado, o empleados desleales entre otros.

32. Seguridad: Todo incumplimiento relacionado con las instalaciones de protección contra incendios, así como del diseño, instalación y mantenimiento de los sistemas de protección activa contra incendios. De la misma manera, todo incumplimiento relativo a la realización y la prestación por personas privadas, físicas o jurídicas, de actividades y de los servicios de seguridad privada suscrita para las instalaciones de RSI.

33. Telecomunicaciones: Conductas que atentan contra la Ley de Telecomunicaciones de 11/2022 como pueden ser entre otros, realizar interferencias internacionales en los sistemas de telecomunicaciones sin autorización, interceptación o acceso ilegal a comunicaciones electrónicas sin consentimiento, utilización fraudulenta de servicios de telecomunicaciones, no cumplir con las obligaciones de confidencialidad y protección de datos establecidos en esta norma, realizar actividades de spam o envío masivo de mensajes no solicitados a través de medios electrónicos, así como no cumplir con las normas de calidad del servicio establecidos en la ley.

34. Tributario: Conductas que atentan contra la normativa tributaria como pueden ser las siguientes acciones entre otras, evasión de impuestos, elusión fiscal, fraude fiscal, ocultación de ingresos o bienes, uso de sociedades pantalla para ocultar la propiedad real de bienes o ingresos, así como prácticas de precios de transferencia.

35. Otros.

– CANAL INTERNO INFORMÁTICO –

¿QUÉ ES UN CANAL INTERNO INFORMÁTICO?

El Canal Interno Informático es el medio más habitual para recibir Comunicaciones o denuncias.

Permite la presentación de denuncias escritas o mediante grabaciones de audio que distorsionan su voz para evitar que sea identificada. En ambos casos, podrá acompañar a su denuncia archivos o grabaciones de audio/video.

A continuación, le daremos a conocer la forma en que funciona el Canal del Sistema de Información (o canal interno de información) implantado por RSI.

¿CÓMO PUEDO ACCEDER AL CANAL INTERNO?

Puede accederse al Canal a través de la web corporativa de RSI, donde encontrará este enlace: https://www.ruralserviciosinformaticos.com/cms/estatico/bl/rsi/web/es/rsi/html/canal-denuncias.html

En la página de inicio del canal encontrará la política de privacidad, la presente Guía de uso del canal.

Para acceder al formulario de denuncias es imprescindible marcar que se han leído, comprendido y aceptado los documentos indicados.

Una vez dentro, el canal le va a solicitar que nos indique:

1. El tipo de Comunicación que se quiere realizar y si considera que es necesario darle una respuesta urgente.
2. La relación que Usted mantiene con RSI.
3. La normativa o conducta susceptible de denuncia que considera que se puede haber vulnerado. Para facilitarle la Comunicación, podrá seleccionar la casilla correspondiente en el listado que el Canal pone a su disposición, que coincide con el que le hemos indicado en el Punto 3 de esta Guía.
4. Asimismo, deberá introducir una contraseña ideada para la ocasión, que deberá repetir para seguir avanzando. Posteriormente a que la herramienta te remita tu contraseña, podrás cambiarla o actualizarla.

AL FORMULAR UN COMUNICACIÓN, ¿DEBO INDENTIFICARME OBLIGATORIAMENTE?

A continuación, deberá seleccionar el modo en que desea realizar la Comunicación, que podrá ser:

- Anónima. De este modo no se le solicitará ningún dato personal. Como no le podremos remitir ninguna notificación, para informarse sobre el estado de su denuncia deberá Usted acceder al Canal con el usuario y contraseña que le habremos asignado.
- Confidencial. De este modo Usted nos indicará sus datos personales y recibirá avisos y notificaciones en el teléfono, correo electrónico o dirección postal que nos haya indicado.

AL FORMULAR UNA COMUNICACIÓN, ¿CÓMO PUEDO EXPONER LOS HECHOS QUE QUIERO COMUNICAR?

Una vez escogida la forma de presentar la Comunicación, deberá ir cumplimentando los diferentes campos, obligatorios u opcionales, que el formulario de comunicaciones la solicite.

El sistema también cuenta con un apartado para dejar su Comunicación grabada en formato audio.

Con independencia que formule su denuncia por escrito o mediante audio, también encontrará incorporado un apartado para adjuntar archivos y grabaciones de audio o video.

SOLICITUD DE COMUNICACIÓN MEDIANTE REUNIÓN PERSONAL

Una vez ha accedido a nuestro Canal del Sistema de Información, Usted también podrá indicar que desea una reunión presencial.

Deberá reflejar, también, su preferencia en cuanto al horario de realización y sus datos de contacto.

Deberá indicar una dirección de correo electrónico o teléfono por medio de la cual se le pueda notificar el lugar, día y hora para su celebración.

Se le responderá fijando una fecha para la reunión dentro de los siete días naturales siguientes a su solicitud.

UNA VEZ HAYA FORMULADO MI COMUNICACIÓN, ¿PUEDO VOLVER A ACCEDER A LA MISMA?

El Canal del Sistema de Información asigna automáticamente a su usuario una que Usted deberá recordar, pues es necesaria junto a su usuario, para poder acceder a su Comunicación en el canal.

Con estas credenciales, Usted podrá consultar y anular la Comunicación que haya realizado, desde el momento de su presentación, salvo que el órgano encargado de las comunicaciones de RSI ordene su bloqueo en aplicación de la normativa sobre protección de datos personales.

Debe tener presente que la anulación de su Comunicación no implicará la no tramitación, aunque el órgano encargado de las comunicaciones será conocedor de su voluntad de desistir y la tendrá en cuenta.

– ENTREVISTA PERSONAL CON EL ÓRGANO ENCARGADO DE LAS COMUNICACIONES –

La entrevista personalizada es un procedimiento de comunicación de infracciones mediante el cual Usted puede hacer su Comunicación de forma presencial ante los responsables del órgano encargado de las comunicaciones.

SOLICITUD DE REUNIÓN

Usted puede solicitar la reunión con los responsables:

1. A través del Canal Interno Informático
2. Solicitándolo directamente al órgano de comunicaciones, bien mediante llamada telefónica (934 155 421) o mediante un correo electrónico remitido a bonatti@bonattipenal.com.

ACUSE DE RECIBO Y CONVOCATORIA DE LA REUNIÓN PRESENCIAL

En un plazo no superior a 7 días recibirá una notificación del órgano de comunicaciones acusando recibo a su solicitud e informándole:

a. Que si Usted opta por mantener la entrevista personalizada no vamos a poder mantener su anonimato y que en RSI existen otro Canales que aseguran dicho anonimato.
b. Que por imperativo legal la entrevista debe ser grabada o transcrita, de modo que si Usted no va a prestar su consentimiento no podremos recoger su Comunicación por este Canal, pudiendo Usted optar por el Canal del Sistema de Información que permiten las Comunicaciones anónimas.
c. Que Usted podrá leer el acta de la reunión y podrá hacer observaciones a su contenido, y que si esta es video-grabada la custodiaremos en un lugar y mediante un sistema seguro.

d. Para mayor garantía, Usted recibirá en dicho correo una copia de la Política de Privacidad del SII, así como de esta Guía.
e. En ese correo recibirá Usted el lugar y hora de la entrevista, que se fijará atendiendo a las indicaciones que Usted nos haya formulado en su solicitud.

DESARROLLO DE LA REUNIÓN

Al inicio de la entrevista, el órgano de comunicaciones volverá a informarle de los contenidos del correo de acuse de recibo y recogeremos su aceptación expresa por escrito, si la entrevista va a ser objeto de transcripción o al inicio de la grabación si va a ser video-grabada.

Al finalizar la entrevista Usted podrá revisar el acta de la reunión o visionar la videograbación con la finalizad de aceptar su contenido o bien hacer las aclaraciones o rectificaciones que considere necesarias.

– PROTECCIÓN DE LOS INFORMANTES –

A continuación, le exponemos algunos aspectos clave de la protección que le interesan como informante y que ofrecemos en RSI a través de nuestro Canal del Sistema de Información o SII:

¿QUIÉN ES UNA PERSONA INFORMANTE ESPECIALMENTE PROTEGIDA?

“Informante” es el término que se recoge 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 para identificar a las personas que informan sobre infracciones y acceden a un estatuto especial de protección legal.

Según dicha Ley, no todas las personas que formulan una Comunicación tienen el reconocimiento legal de Informantes, este se objetiva en las personas que mantienen relaciones laborales o profesionales con RSI, en concreto se consideran informantes especialmente protegidos los que indicamos en el apartado 4 de nuestra “Política del Sistema Interno de Información” y, que exponemos a continuación:

a. Las personas que trabajan o hayan trabajado para RSI.

b. Los autónomos que mantengan con RSI cualquier clase de relación de prestación de servicios.

c. Socios cooperativos, participes, personas que integran el Consejo de Administración o la Alta Dirección.

d. Cualquier otra persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

e. Voluntarios, trabajadores en periodos de formación con independencia de que perciban o no una remuneración, así como a aquellos cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones se haya obtenido durante el proceso de selección o de negociación precontractual.

Se asimilan a los informantes especialmente protegidos las siguientes personas:

1. Los representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo a la Persona Informante.

2. Las personas físicas que, en el marco de la organización en la que preste servicios la Persona Informante, asistan al mismo en el proceso,

3. Las personas físicas que estén relacionadas con la Persona Informante y que puedan sufrir represalias, como compañeros de trabajo o familiares de la Persona Informante.

4. Las 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 que le permita tener capacidad de influencia.

¿CÓMO SE ACCEDE A LA CONSIDERACIÓN LEGAL DE INFORMANTE?

Usted tendrá la consideración de "Informante" y el derecho a la protección que establece la Ley 2/2023 cuando se den las siguientes condiciones que exponemos de forma resumida a continuación:

- Que comunique información sobre las infracciones comprendidas en el Punto 3.2 , del listado recogido en esta Guía.
- Que nos comunique la información a través de alguno de los Canales que le hemos presentado en esta Guía.
- Cuando Usted tenga pruebas, o bien cuando tenga sospechas o motivos razonables para pensar que la información que nos transmite es veraz, aun cuando Usted no tenga pruebas concluyentes de los hechos que nos comunica.

Debemos advertirle que no va a tener derecho a la protección de la Ley si la información que nos comunica:

- Ya ha sido comunicada antes por otro Canal o por otro Informante y hemos rechazado su admisión o la hemos investigado y archivado por no ser relevante.
- Es información relativa a conflictos personales entre Usted y las personas denunciadas o entre las personas denunciadas y un tercero, en cuyo caso se debe Usted dirigir a las autoridades policiales o judiciales competentes, dado que RSI no tiene ninguna capacidad de intervención en estos casos.
- Se trate de informaciones que ya sean públicas o conocidas en RSI, o bien se trate de rumores que se difunden dentro o fuera de RSI. Dicho de otro modo, la Información que podemos admitir es aquella que Usted haya obtenido directamente, por hechos que ha visto, oído o documentos que han llegado a su poder.
- Informaciones que no tengan que ver con las infracciones, incumplimientos o contravenciones recogidas en el Punto 3 de esta Guía.

¿QUÉ PROTECCIÓN TENGO SI NO SOY UN INFORMANTE ESPECIALMENTE PROTEGIDO Y REALIZO UNA COMUNICACIÓN?

Los Informantes que no están especialmente protegidos son todas aquellas personas que realizan una Comunicación a través de los Canales Internos de RSI y:

- Son clientes, usuarios, autoridades, competidores o cualquier otra persona no contemplada como "especialmente protegida".
- Que comunique información sobre las infracciones comprendidas en el Punto 3 de esta Guía.

Para RSI es irrelevante que la Persona Informante sea o no sea "especialmente protegida", ya que daremos a todas las personas que informen el más alto grado de protección.

Ofreceremos exactamente la misma protección a cualquier persona que informe sobre cualquier irregularidad, porque para nosotros todas son exactamente igual de importantes. Pero la Ley 2/2023 las excluye de su régimen de protección, y no contarán con el amparo de las Autoridades Administrativas Independientes.

¿QUIÉN SE VA A RESPONSABILIZAR DE MI PROTECCIÓN?

El Responsable del Sistema Interno de Información en RSI es el Comité del Sistema Interno de Información siendo el máximo responsable y garante de la protección de la Persona Informante frente represalias por parte de cualquier miembro de la organización o ajeno a la misma. Para ello, el Órgano de Gobierno de RSI le ha otorgado todas las facultades de decisión necesarias dentro de RSI.

En su labor, el Responsable del SII cuenta con un órgano interno responsable para la protección de la Persona Informante y con un órgano responsable de las comunicaciones para la gestión de los Canales Internos.

Como informante, Usted tiene derecho a recibir protección en los términos que se exponen a continuación.

¿HASTA DÓNDE LLEGA MI PROTECCIÓN?

RSI ha prohibido cualquier acto que pueda considerarse represalia, incluidas las amenazas de represalia y las tentativas de represalia, contra cualquier persona que formule una Comunicación o denuncia.

¿QUÉ ES UNA REPRESALIA?

Todo comportamiento, acción u omisión prohibida por la ley, o que, de forma directa o indirecta, conlleve un trato desfavorable que sitúe a las personas que los sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, como consecuencia de su condición de informantes, o por haber usado los Canales Internos o haber realizado una revelación pública.

Son ejemplos de represalias:

- **En el ámbito laboral, profesional o empresarial, conductas como la 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 Usted tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido o la denegación de formación.**
- **Los daños a sus bienes, las pérdidas económicas deliberadas, coacciones, intimidaciones, actos de acoso u ostracismo.**
- **Los ataques a su reputación, daños a su honor, menciones a su salud física o mental, evaluaciones o referencias negativas referentes a su desempeño laboral o profesional, asi como la inclusión en listas negras o la difusión de información negativa o falsa en su sector profesional o empresarial con el ánimo de impedirle el acceso al empleo o la contratación de obras o servicios.**
- **Otras conductas discriminatorias, desfavorables o injustas, como la denegación o anulación arbitraria de una licencia o permiso.**

¿TODOS LOS ACTOS ANTERIORES SE VAN A CONSIDERAR REPRESALIAS?

NO, sólo cuando el acto sea como consecuencia de su condición de informantes, o por haber usado los

Canales Internos o haber realizado una revelación pública.

Si las medidas anteriores se llevaran a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral o reguladora del estatuto del empleado público correspondiente, por circunstancias, hechos o infracciones acreditadas, y ajenas a la presentación de la Comunicación no van a ser consideradas como una represalia.

¿LA PROTECCIÓN ABARCA SOLO A LA PERSONA INFORMANTE?

No, en RSI extendemos la protección a las personas y entidades establecidas en el Apartado 4 de nuestra "Política del Sistema Interno de Información", que le acompañamos con esta Guía.

En cualquier caso, es importante que sepa que no sólo le protegemos a Usted, sino también a aquellas personas compañeras de trabajo o familiares que estén relacionadas con Usted y a las empresas o entidades para las que Usted trabaja o en las que tenga una participación empresarial relevante.

¿CÓMO RESPONDE RSI FRENTE A UNA REPRESALIA?

Los actos que tengan por objeto impedirle o dificultarle la presentación de su Comunicación, así como los que constituyan represalia o causen discriminación tras la presentación de aquellas, son nulos de pleno derecho y darán lugar a que RSI anule dichos actos y adopte medidas correctoras disciplinarias o de responsabilidad para aquellos directivos, empleados u otras personas de la organización que las comentan, sin perjuicio de que comunique tales conductas a la Autoridad Administrativa Independiente para que les imponga las correspondientes sanciones.

¿CÓMO SE VA A ASEGURAR MI PROTECCIÓN?

Usted estará bajo la protección del Responsable del SII desde el momento en que su Comunicación sea admitida a trámite por el órgano responsable de comunicaciones y se regirá por los siguientes principios:

- El Responsable del SII o el órgano responsable de la protección establecerá con Usted un canal de comunicación (mediante correo electrónico o teléfono) con la finalidad de poder conocer rápidamente si Usted sufre algún tipo de represalia o consecuencia tras haber realizado la Comunicación.
- Si Usted lo necesita, el órgano responsable de la protección le ofrecerá soporte y asesoramiento sobre las consecuencias de su Comunicación, informándole especialmente sobre aquellas medidas de protección o apoyo que únicamente ofrecen las Autoridades de Protección a la Persona Informante competentes, ayudándole en su caso a obtener el reconocimiento como Informante por parte de la AAI.
- RSI ha establecido un procedimiento de protección a la Persona Informante para asegurar su salvaguarda y la confidencialidad de su identidad en todo momento. Asimismo, el responsable del SII o, el órgano responsable de la protección, velarán en todo momento para asegurarse que se cumple y no se filtra ningún dato que revele su identidad.
- El Responsable del SII o el órgano responsable de la protección están autorizados por el órgano de gobierno de RSI para adoptar cuantas medidas considere adecuadas para asegurar la salvaguarda e indemnidad de la Persona Informante.
- Si Usted lo precisa, le ayudaremos a gestionar cualquier solicitud de protección, ayuda u otro recurso que dependa de la Autoridad Administrativa Independiente para la Protección de las Personas Informantes, con la que RSI colaborará en todo momento a través del Responsable del SII para velar por su seguridad y tranquilidad.

Vd. podrá comunicar en cualquier momento toda clase de incidencias relativas a la información comunicada y, especialmente, recabar el amparo frente represalias (incluso aun cuando las mismas constituyan tan solo tentativas o amenazas de sufrirlas).

¿CÓMO VAMOS A PROTEGER SU IDENTIDAD?

a. Usted tiene derecho a que su identidad no sea revelada a terceras personas.

b. Nuestro Sistema Interno de Información ha implantado en todos los niveles de RSI medidas técnicas y organizativas adecuadas para preservar su identidad y garantizar la confidencialidad de todos los datos, identidades, archivos e informaciones que nos facilite.

c. El Responsable del SII o el órgano responsable de la protección velan por la eficaz implantación de las indicadas medidas, su revisión y mejora continua.

d. Por imperativo legal, su identidad debe informarse a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora, cuando esta Autoridad adopte una resolución judicial motivada.

e. Los datos sobre su identidad se entregarán directamente a la Autoridad Judicial que haya adoptado la decisión, quien asumirá su gestión y, en su caso, la protección de su persona en el ámbito judicial.

f. Si nos llegara un requerimiento judicial solicitando revelar su identidad que cumpla con todos los requisitos legales, le notificaremos este hecho antes de revelar su identidad a la Autoridad Judicial, excepto en el caso que la resolución judicial nos lo prohíba expresamente, lo que puede ocurrir, por ejemplo, si la investigación judicial ha sido declarada secreta.

– CANALES EXTERNOS Y AUTORIDADES DE PROTECCIÓN A LOS INFORMANTES –

Como informante, Vd. puede dirigir directamente Comunicaciones a la Autoridad Independiente de Protección de la Persona Informante, (en adelante, A.A.I.) y respecto a ello podrá:

1. 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.
2. Formular la Comunicación verbalmente o por escrito.
3. Indicar un domicilio, correo electrónico o lugar seguro donde recibir las comunicaciones que realice la A.A.I. a propósito de la investigación.
4. Renunciar, en su caso, a recibir notificaciones de la A.A.I.
5. Comparecer ante la A.A.I., por propia iniciativa o cuando sea requerido por esta, siendo asistido, en su caso y si lo considera oportuno, por abogado.
6. Solicitar a la A.A.I. 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.
7. Ejercer los derechos que le confiere la legislación de protección de datos de carácter personal.
8. Conocer el estado de la tramitación de su denuncia y los resultados de la investigación.

MEDIDAS DE APOYO

La Autoridad Independiente de Protección de la Persona Informante, A.A.I. podrá adoptar en su favor las siguientes medidas de apoyo:

- Información y asesoramiento completos e independientes, fácilmente accesibles y gratuitos, sobre los procedimientos y recursos a su disposición.
- Protección frente a represalias y derechos de la persona afectada.
- Asistencia efectiva ante cualquier autoridad pertinente implicada en su protección frente a represalias, incluida la certificación de que pueden acogerse a protección al amparo de la presente ley.
- Asistencia jurídica en los procesos penales y en los procesos civiles transfronterizos de conformidad con la normativa comunitaria.
- Apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la Autoridad Independiente de Protección de la Persona Informante, A.A.I. tras la valoración de las circunstancias derivadas de la presentación de la Comunicación.

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

– CONSECUENCIAS DE LA COMUNICACIÓN INVERAZ O ILÍCITA –

¿QUÉ ES INFORMACIÓN NO VERAZ O ILÍCITA?

La Ley sanciona de forma expresa el hecho de informar a través de un Canal Interno o Externo sobre hechos que la Persona Informante sabe que no son ciertos o sobre hechos cuya información se ha obtenido cometiendo algún tipo de delito, de modo que le recomendamos que se abstenga de hacer cualquier Comunicación que tenga su origen en este tipo de conductas.

Por información no veraz debemos entender:

- Información inventada.
- Información tergiversada o manipulada para que parezca una infracción cuando no lo es.
- Información presentada parcialmente, omitiendo de forma deliberada datos o hechos que demuestran que no se produjo una infracción.

- Información acompañada de archivos o documentos que han sido objeto de cualquier clase de alteración o en los que se atribuye la intervención de personas que no participaron en los mismos.

Por información obtenida de forma delictiva hacemos referencia a:

- Que los archivos, documentos u otras pruebas se han obtenido mediante su robo, hurto, allanamiento de domicilios o empresas, entrega bajo coacciones, agresión física o bien hackeando o vulnerando de cualquier modo las medidas de seguridad de los sistemas tecnológicos.
- Que las manifestaciones de las personas denunciadas se hayan obtenido bajo coacciones, agresión física, retención ilegal, chantaje o bien hackeando sus sistemas informáticos o vulnerando la privacidad de sus comunicaciones telefónicas, correos informáticos o comunicaciones postales.
- Que las pruebas se hayan obtenido mediante grabaciones con micrófonos o cámaras ocultas en espacios protegidos por el derecho a la privacidad de las personas.

No se considerará que Usted ha obtenido la información ilícitamente:

- Cuando las grabaciones audiovisuales se corresponden a llamadas o videoconferencias en las que Usted interviene personalmente.
- Cuando la información ha llegado a su poder como consecuencia de su actividad laboral y/o profesional, aun en el supuesto en que haya firmado cláusulas de confidencialidad u otras restricciones legales a su divulgación, si bien Usted solo puede usar la información para hacer la Comunicación o denuncia, absteniéndose de divulgarla a terceras personas ajenas a la gestión de los Canales Internos o Externos donde hace la Comunicación.

¿ESO SIGNIFICA QUE NO PUEDO HACER UNA COMUNICACIÓN BASADA EN SOSPECHAS?

Sí podrán realizar comunicaciones basadas en sospechas y, además es necesario que las haga.

No obstante, si Usted va a basar su Comunicación en sospechas o indicios, exponga con claridad en qué indicios o sospechas se fundamenta su convicción de que se ha cometido, se está cometiendo o se puede cometer una irregularidad.

Explique con claridad lo que sabe con certeza y lo que se basa en conclusiones o conjeturas sobre las que no tiene una prueba concluyente.

Si va a presentar algún documento cuya autenticidad no tenga probada al 100%, adviértalo en la Comunicación, indicando su origen y cómo lo ha obtenido.

¿QUÉ PUEDE OCURRIR SI EL ÓRGANO RESPONSIBLE DE LAS COMUNICACIONES DETECTA QUE USTED HA HECHO UNA COMUNICACIÓN NO VERAZ U OBTENIDA DED FORMA ILÍCITA?

Si el órgano responsable de las comunicaciones llega a tener sospechas fundadas sobre su Comunicación se lo notificará abiertamente para requerirle que las aclare con carácter previo a adoptar cualquier otra medida.

En el supuesto que Usted no responda al requerimiento, o las explicaciones que nos ofrezca no despejen las dudas o sospechas que se ciernen sobre su Comunicación, el órgano responsable de las comunicaciones procederá a archivarla, informando de los hechos al Responsable del SII.

20. CONSECUENCIAS DE LA COMUNICACIÓN E INFORMACIÓN INVERAZ O ILÍCITA

1. Si se considera que puede haber mala fe, imprudencia temeraria o indicios de delito en la obtención de la información o en su Comunicación, el Responsable del SII:
2. Informará al órgano de gobiernocon la finalidad de proceder a la presentación de la correspondiente denuncia ante la Fiscalía General del Estado.
3. Informará a las personas denunciadas que hayan sido víctimas de los hechos para que puedan instar acciones judiciales contra Usted, si así lo consideran.
4. Autorizará el bloqueo y conservación de la Comunicación y toda la documentación acompañada, que quedará a disposición de los Juzgados y Tribunales que investiguen y juzguen los hechos.
5. Informará de los hechos a la Autoridad Administrativa Competente para que pueda instar el procedimiento sancionador por infracción muy grave al amparo del artículo 63.1f) de la Ley 2-2023 sancionado con multas que van desde 30.001 hasta los 300.000 euros.
6. Remitirá informe de los hechos al departamento interno de RSI que corresponda para que proceda a instruir el correspondiente procedimiento sancionador interno.

Si se considera que los hechos son no veraces, pero no hay mala fe, imprudencia temeraria o indicios de delito en su comportamiento, se procederá a la destrucción inmediata de la información y los documentos acompañados.