

**Política relativa al
Sistema Interno de Información
y la Defensa del Informante de
BOUTIQUE DEL SEGURO BALEAR
CORREDURÍA DE SEGUROS, S.L.**

Contenido

1. Principios

2. Objetivos

3. Definiciones

4. Hechos denunciables

5. Informantes

6. Responsable del Sistema

7. Procedimiento de Gestión de Comunicaciones

7.1. Recepción de la comunicación (Canales Internos de Información)

7.2. Evaluación de la comunicación (Canales Internos de Información)

7.3. Tratamiento de la comunicación (Canales Internos de Información)

7.4. Conclusión de la comunicación (Canales Internos de Información)

8. Revelación pública

9. Medidas de protección

9.1. Medidas contra las represalias

9.2. Medidas de apoyo

9.3. Medidas frente a la responsabilidad del informante

9.4. Medidas para la protección de las personas afectadas

10. Protección de datos

10.1. Régimen jurídico del tratamiento de datos personales

10.2. Licitud de los tratamientos de datos personales

10.3. Información sobre protección de datos personales y ejercicio de derechos

10.4. Tratamiento de datos personales en el Sistema Interno de Información

10.5. Preservación de la identidad del informante y de las personas afectadas

11. Información, formación y mejora continua

1. PRINCIPIOS

Los principios fundamentales que en BOUTIQUE DEL SEGURO BALEAR CORREDURÍA DE SEGUROS, S.L. promovemos a través de nuestra **Política relativa al Sistema Interno de Información y la Defensa del Informante** son:

- **El respeto a las leyes y normas internas de la entidad.**
Por parte de todas las personas que forman parte de la misma y el compromiso de estas de informar si detectan que alguien no lo hace.
- **El respeto a la libertad de expresión y de información.**
Los derechos a comunicar y a recibir informaciones, reconocidos tanto en la Constitución Española (artículo 20) como en la Carta de los Derechos Fundamentales de la Unión Europea (artículo 11), son la base de nuestro Sistema Interno de Información.
- **La buena fe de las personas informantes.**
Esto es, tener una conciencia honesta a la hora de comunicar que se ha producido o puede producirse alguna irregularidad dentro, por o para la entidad.
- **El comportamiento cívico.**
Que evite realizar comunicaciones falsas o tergiversadas, así como aquellas que contengan información obtenida de manera ilícita.
- **El respeto a la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones.**
Como pilares para el correcto funcionamiento de nuestro Sistema Interno de Información.
- **La debida diligencia a la hora de actuar ante la comunicación de una posible irregularidad.**
Como compromiso tanto para las personas informantes como para la propia entidad, de modo que fortalezcamos nuestra confianza organizacional.

2. OBJETIVOS

Este documento se aprueba con el fin de alcanzar los siguientes objetivos:

- Detectar las posibles irregularidades cometidas dentro, por o para la entidad, con el fin de actuar de forma diligente y eficaz en el seno de la misma y de paralizar las posibles consecuencias perjudiciales.
- Prevenir y minimizar los daños a la entidad, incluida la responsabilidad legal, las pérdidas financieras y el daño en su reputación, al permitir la detección temprana de las irregularidades y su corrección.
- Prevenir y minimizar el daño al interés público, incluyendo la salud pública, los derechos humanos y el medio ambiente.
- Proteger a las personas que informen sobre las acciones u omisiones recogidas en el artículo 2 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.

- Garantizar la confidencialidad de la información, así como el anonimato de las personas que así lo elijan a la hora de informar de una posible infracción.
- Promover la cultura de la información, la confianza, la transparencia y la rendición de cuentas como parte de la ética e integridad de la entidad con el fin de prevenir cualquier infracción o irregularidad.

3. DEFINICIONES

Infracción: acción u omisión que sea ilícita y esté relacionada con los actos y ámbitos recogidos en el punto 4 (Ámbito de aplicación material).

Información sobre infracciones: comunicación de las acciones u omisiones ilícitas, incluidas las sospechas razonables, sobre irregularidades reales o potenciales, que se hayan producido o que probablemente puedan producirse en una entidad en la que trabaje o haya trabajado la persona informante o en otra entidad con la que esté o haya estado en contacto con motivo de su trabajo, y sobre los intentos de ocultar los hechos.

Información: comunicación de una infracción, puede ser verbal o por escrito.

Información interna: comunicación de una infracción, realizada a través de los canales establecidos por la entidad, puede realizarse verbalmente o por escrito.

Información externa: comunicación de una infracción, realizada a través de los canales establecidos por las autoridades competentes, puede ser verbal o por escrito.

Revelación pública o revelar públicamente: puesta a disposición del público de información sobre infracciones.

Informante: persona física que comunica o revela públicamente información sobre infracciones.

Contexto laboral: entorno de trabajo, presente o pasado, a través del cuales, con independencia de la naturaleza de las actividades realizadas, una persona puede obtener información sobre infracciones y en el que podría sufrir represalias si comunicase dicha información.

Persona afectada: persona física o jurídica a la que, en la información sobre infracciones o revelación pública, se le atribuye dicha infracción o con la que se le asocia.

Represalia: toda acción u omisión que esté prohibido por la ley, o que, de forma directa o indirecta, suponga un trato desfavorable que sitúe a la persona que la sufra en desventaja particular con respecto a otra en el contexto laboral o profesional, solo por su condición de informante o por haber realizado una revelación pública.

Seguimiento: toda acción emprendida por el destinatario de una información sobre infracciones o por cualquier autoridad competente a fin de valorar la exactitud de la información y, en su caso, de resolver la infracción denunciada, incluso a través de medidas como

investigaciones internas, investigaciones, acciones judiciales, acciones de recuperación de fondos o el archivo del procedimiento.

Respuesta: comunicación facilitada al informante sobre las medidas previstas o adoptadas para seguir su denuncia y sobre los motivos de tal seguimiento.

Autoridad competente: toda autoridad nacional o autonómica designada para recibir información sobre infracciones, adoptar medidas de protección, tramitar procedimientos, imponer sanciones y dar respuesta a los informantes.

4. HECHOS DENUNCIABLES

Nuestro Sistema Interno de Información tiene, como prioridad, recibir comunicaciones sobre las infracciones recogidas 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. Estas son:

- 1) Cualesquiera acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea. Estas son:
 - a) Las relativas a los ámbitos siguientes:
 - Contratación pública.
 - Servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo.
 - Seguridad de los productos y conformidad.
 - Seguridad del transporte.
 - Protección del medio ambiente.
 - Protección frente a las radiaciones y seguridad nuclear.
 - Seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales.
 - Salud pública.
 - Protección de los consumidores.
 - Protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información.
 - b) Las que afecten a los intereses financieros de la Unión tal como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (T.F.U.E.) y tal como se concretan en las correspondientes medidas de la Unión.
 - c) Las relativas al mercado interior, tal como se contemplan en el artículo 26, apartado 2, del T.F.U.E., incluidas las infracciones de las normas de la Unión 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 a prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable del impuesto sobre sociedades.
- 2) 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.

No obstante, por nuestro compromiso con la ética empresarial y teniendo en cuenta los desarrollos legislativos tanto a nivel nacional como europeo, nuestra entidad se reserva la posibilidad de utilizar nuestro Sistema Interno de Información con el fin de recibir comunicaciones sobre infracciones de otra índole, teniendo siempre presente los principios y objetivos recogidos en este documento.

Si bien el artículo 35.1.d) de la Ley 2/2023 establece que las personas que comuniquen o revelen infracciones que se refieran a acciones u omisiones no comprendidas en los apartados 1 y 2 anteriores, no tendrán derecho a la protección recogida en esta Ley.

5. INFORMANTES

Nuestro Sistema Interno de Información está dirigido a proteger a aquellas personas que hayan obtenido información sobre infracciones en un contexto laboral o profesional, comprendiendo en todo caso:

- 1) Las personas que tengan la condición de empleados públicos o trabajadores por cuenta ajena.
- 2) Los autónomos.
- 3) Los accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa, incluidos los miembros no ejecutivos.
- 4) Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

Asimismo, podrán realizar comunicaciones las personas que hayan obtenido la información sobre infracciones en el marco de una relación laboral o estatutaria ya finalizada, voluntarios, becarios, trabajadores en periodos de formación con independencia de que perciban o no una remuneración, así como a aquellos cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.

6. RESPONSABLE DEL SISTEMA

Con el fin de garantizar que el Sistema Interno de Información se ajuste a las recomendaciones de este documento, la dirección de la entidad designará una persona como responsable, en adelante Responsable del Sistema.

Esta persona realizará sus funciones de forma independiente y autónoma del resto de los órganos de la entidad, sin recibir instrucciones de ningún tipo y contará con todos los medios personales y materiales necesarios para desempeñarlas. Además, se inhibirá en caso de

conflicto de intereses, menoscabo de su confianza o merma de la imparcialidad. No obstante, rendirá cuentas a la dirección de la entidad sobre el funcionamiento del propio Sistema.

7. PROCEDIMIENTO DE GESTIÓN DE COMUNICACIONES

Toda comunicación con información sobre infracciones o posibles infracciones recibida a través de nuestro Sistema Interno de Información pondrá en marcha nuestro Procedimiento de Gestión de Comunicaciones, conforme al artículo 9 de la Ley 2/2023.

Las comunicaciones se enviarán a través de cualquiera de los Canales Internos de Información creados para tal fin, siendo el Canal principal el habilitado en la url:

grupbsb.tucanaseguro.com

Así como información sobre la Autoridad Independiente de Protección del Informante (A.A.I.) y el Canal Externo de Información gestionado por ella.

Nuestros Canales Internos ofrecen un alto grado de confidencialidad y uno de ellos garantiza totalmente el anonimato del informante. Además, nuestro procedimiento está basado en la ISO 37002, y tiene como fundamentos la confianza, la imparcialidad y la protección.

Estos fundamentos conforman el marco de referencia para cada una de las fases por las que atraviesa la comunicación, las cuales se desarrollarán con la diligencia debida y son: recepción, evaluación, tratamiento y conclusión.

7.1. Recepción de la comunicación (Canales Internos de Información)

Paso 1

Registrar la información en una base de datos segura y de acceso restringido exclusivamente al personal autorizado.

Paso 2

Enviar al informante acuse de recibo en un plazo máximo de siete días naturales desde la fecha de recepción, a menos que con ello se pueda comprometer la confidencialidad de la comunicación.

7.2. Evaluación de la comunicación

Paso 3

Triar la información recibida, de forma que se determine el ámbito al que afecta y se compruebe si hace referencia a alguno de los hechos denunciados recogidos en el apartado 4 de este documento, en cuyo caso, la gestión de la comunicación, dependerá del Responsable del Sistema.

Paso 4

Decidir, en un plazo máximo de diez días hábiles desde la recepción de la comunicación, si:

a) No se admite por:

- Carecer de verosimilitud.
 - No hacer referencia a alguno de los hechos denunciados recogidos en el apartado 4 de este documento, en cuyo caso se podrá derivar a la persona o departamento con autoridad para actuar en el ámbito afectado.
 - Carecer de fundamento.
 - Existir indicios razonables de haberse obtenido mediante la comisión de un delito.
 - No contener información nueva y significativa sobre procesos anteriores. La inadmisión se comunicará en un plazo máximo de los cinco días hábiles siguientes a tomar dicha decisión.
- b) Se admite. En cuyo caso se le comunicará al informante en un plazo máximo de los cinco días hábiles siguientes a tomar dicha decisión. Y el Responsable del Sistema, con el fin de ayudar a priorizar las actuaciones, asignará un nivel de gravedad (alta-media-baja).
- c) Se remite con carácter inmediato la información al Ministerio Fiscal cuando los hechos pudieran ser indiciariamente constitutivos de delito o a la Fiscalía Europea si los hechos afectan a los intereses financieros de la Unión Europea.
- d) Se remite la información a la autoridad, entidad u organismo competente para su tramitación.

7.3. Tratamiento de la comunicación

Paso 5

Instruir mediante actuaciones encaminadas a comprobar la verosimilitud de los hechos contenidos en la información.

Paso 6

Evaluar el riesgo de perjuicios, para el informante, otras personas involucradas y la propia entidad.

Paso 7

Establecer las medidas de protección necesarias para minimizar los perjuicios.

Paso 8

Realizar una investigación imparcial y diligente, respetando la presunción de inocencia y el honor de las personas afectadas, así como las disposiciones sobre protección de datos. Además, se llevará a cabo con la previsión de:

- a) Solicitar al informante datos adicionales si se considera necesario.
- b) Informar, conforme a derecho, a las personas afectadas a las que se les atribuyan las acciones u omisiones referidas en la comunicación, quienes asimismo tienen derecho a ser oídas en cualquier momento, con el fin de conocer su versión de los hechos y aportar las pruebas que considere adecuadas y pertinentes, en tiempo y forma que se considere oportuno para garantizar el buen fin de la investigación. En

ningún caso se facilitará la identidad del informante ni se dará acceso a la comunicación.

- c) Garantizar siempre la confidencialidad, incluso si la comunicación ha sido remitida por canales diferentes a los Canales Internos de Información establecidos o a través del personal distinto al responsable de su gestión.

7.4. Conclusión de la comunicación

Paso 9

Emitir un informe, tras dar por concluidas todas las actuaciones, con una exposición de:

- a) Los hechos relatados.
- b) El código de identificación de la comunicación.
- c) La fecha de registro.
- d) El nivel de gravedad de la comunicación a efectos de la prioridad en la tramitación.
- e) Las actuaciones realizadas para comprobar la verosimilitud de los hechos.
- f) Las conclusiones alcanzadas en la investigación y la valoración de las diligencias y los indicios en las que se basan las mismas.
- g) Las recomendaciones oportunas derivadas de las conclusiones expuestas:
 - Propuesta de medidas de protección y apoyo, así como el seguimiento de las mismas.
 - Propuesta de medidas correctivas con el fin de prevenir las mismas irregularidades.
 - Aprendizaje organizacional adquirido durante el proceso, en su caso.

Paso 10

Adoptar alguna de las siguientes decisiones:

- a) Archivo del expediente, hecho que será notificado al informante y, en su caso, a las personas afectadas.
- b) Remisión al Ministerio Fiscal, si el resultado de la instrucción indicase que se aprecian indicios de que los hechos pudieran revestir el carácter de delito, o a la Fiscalía Europea, si el delito afectase a los intereses financieros de la Unión.
- c) Traslado de todo lo actuado a la autoridad competente.
- d) Acuerdo de inicio de un procedimiento disciplinario.

El plazo máximo para cerrar las investigaciones y dar respuesta a la comunicación gestionada es de 3 meses desde la recepción de la misma o de 3 meses y 7 días en caso de no haberse enviado al informante acuse de recibo. Ampliable hasta otros 3 meses si el caso es especialmente complejo.

El Responsable del Sistema podrá, en caso de ser necesario, contar con recursos humanos que colaboren en las labores de gestión de la comunicación. El personal designado deberá comprender, cumplir y aplicar los términos recogidos en este documento.

En determinados casos, y como consecuencia de la complejidad y el alcance de la información, la entidad podrá subcontratar ciertas funciones del Sistema de Gestión de Comunicaciones, como pueden ser la recopilación, el procesamiento, la investigación o la redacción del informe de conclusiones. No obstante, el Responsable del Sistema supervisará dichas funciones y mantendrá la autoridad sobre las mismas.

8. REVELACIÓN PÚBLICA

Conforme al Título V 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, el hecho de poner a disposición del público la información sobre los hechos denunciados recogidos en el apartado 4 de la presente política, le da derecho a la persona que la realice a que se le aplique una serie de medidas de protección, a las que tendrá acceso si:

- a) Tienen motivos razonables para pensar que la información referida es veraz en el momento de la comunicación o revelación, aun cuando no aporte pruebas concluyentes.
- b) La revelación se haya realizado conforme a los requerimientos previstos en la citada ley.
- c) Se ha realizado la comunicación primero por canales internos y externos, o directamente por canales externos, sin que se hayan tomado medidas apropiadas al respecto en el plazo establecido.
- d) Tiene motivos razonables para pensar que, o bien la infracción puede constituir un peligro inminente o manifiesto para el interés público, en particular cuando se da una situación de emergencia, o existe un riesgo de daños irreversibles, incluido un peligro para la integridad física de una persona; o bien, en caso de comunicación a través de canal externo de información, exista riesgo de represalias o haya pocas probabilidades de que se dé un tratamiento efectivo a la información debido a las circunstancias particulares del caso, tales como la ocultación o destrucción de pruebas, la connivencia de una autoridad con el autor de la infracción, o que esta esté implicada en la infracción.

9. MEDIDAS DE PROTECCIÓN

9.1. Medidas contra las represalias

Se prohíbe cualquier tipo de represalia, así como las amenazas de represalia o las tentativas de represalia contra los informantes.

Se consideran represalias:

- a) Suspensión del contrato de trabajo, despido o extinción de la relación laboral o estatutaria, incluyendo la no renovación o la terminación anticipada de un contrato de trabajo temporal una vez superado el período de prueba, o terminación anticipada o anulación de contratos de bienes o servicios, imposición de cualquier medida disciplinaria,

degradación o denegación de ascensos y cualquier otra modificación sustancial de las condiciones de trabajo y la no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido; salvo que estas medidas se llevaran a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral, por circunstancias, hechos o infracciones acreditadas, y ajenas a la presentación de la comunicación.

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

El informante podrá solicitar esta medida incluso si han transcurrido dos años, periodo de tiempo que, excepcionalmente y de forma justificada, la autoridad competente podrá extender.

9.2. Medidas de apoyo

El informante tendrá acceso al siguiente apoyo:

- a) Información y asesoramiento completos e independientes, que sean fácilmente accesibles para el público y gratuitos, sobre los procedimientos y recursos disponibles, protección frente a represalias y derechos de la persona afectada.
- b) Asistencia efectiva por parte de las autoridades competentes ante cualquier autoridad pertinente implicada en su protección frente a represalias.
- c) Asistencia jurídica en los procesos penales y en los procesos civiles transfronterizos de conformidad con la normativa comunitaria.
- d) Apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la Autoridad Independiente de Protección del Informante (A.A.I.) tras la valoración de las circunstancias derivadas de la presentación de la comunicación.

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.

9.3. Medidas frente a la responsabilidad del informante

Cuando un informante realiza una revelación pública con motivos razonables para pensar que la comunicación es necesaria para revelar una infracción se considerará que no ha

violado ninguna restricción de revelación de información, por lo que no se le podrá exigir ninguna responsabilidad. Esta medida incluye a los representantes de las personas trabajadoras, aunque se encuentren sometidas a obligaciones legales de sigilo o de no revelar información reservada.

No incurrirán en responsabilidad respecto de la adquisición o el acceso a la información que revelada siempre que para conseguirla no se haya cometido un delito.

Si el informante se ve inmerso en un proceso judicial, 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, podrá alegar en su descargo haber hecho la revelación pública con el fin de comunicar una infracción, eximiéndole de toda responsabilidad.

9.4. Medidas para la protección de las personas afectadas

Las personas afectadas por la comunicación tienen derecho a la presunción de inocencia, al derecho de defensa y al derecho de acceso al expediente, así como a la misma protección establecida para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

Estas medidas de protección también se aplicarán, en su caso, a:

- a) Las personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso, incluidos los representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante.
- b) Las personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante.
- c) 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 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.

10. PROTECCIÓN DE DATOS

10.1. Régimen jurídico del tratamiento de datos personales

Los tratamientos de datos personales que deriven de la aplicación de esta política se registrarán por lo dispuesto en el RGPD y la LOPD-GDD y tendrán como finalidad la prevención, detección e investigación de infracciones penales.

No se recopilarán datos personales que no sean necesarios para tratar una información específica y, si se recopilan por accidente, se eliminarán inmediatamente. (Principio de proporcionalidad).

10.2. Licitud de los tratamientos de datos personales

El tratamiento es lícito en base a:

1. La aplicación de Ley 2/2023.
2. El cumplimiento de una obligación legal (artículos 6.1.c) del RGPD y 11 de la LOPD-GDD) cuando la entidad debe implementar un Sistema Interno de Información.

En el caso de las categorías especiales de datos personales el tratamiento es lícito por razones de un interés público esencial, conforme a lo previsto en el artículo 9.2.g) del Reglamento (UE) 2016/679.

10.3. Información sobre protección de datos personales y ejercicio de derechos

Cuando los datos personales se obtengan directamente de los interesados se deberá cumplir con el deber de informar (artículos 13 del RGPD y 11 de la LOPD-GDD).

A quienes realicen una revelación pública se les informará, además, de forma expresa, de que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.

Los interesados podrán ejercer los derechos recogidos en el RGPD (artículos 15 a 22).

El hecho de que la persona afectada por la revelación pública ejerciese el derecho de oposición, se presumirá que existen motivos legítimos imperiosos que justifican el tratamiento de sus datos personales.

10.4. Tratamiento de datos personales en el Sistema Interno de Información

El acceso a los datos personales contenidos en el Sistema Interno de Información, que quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente a:

- a) El Responsable del Sistema y a quien lo gestione directamente.
- b) El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.
- c) El responsable de los servicios jurídicos de la entidad u organismo, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.
- d) Los encargados del tratamiento que eventualmente se designen.
- e) El delegado de protección de datos.

El tratamiento de los datos por otras personas, o incluso su comunicación a terceros, será lícito cuando sea necesario para adoptar medidas correctoras en la entidad o tramitar los procedimientos sancionadores o penales que, en su caso, procedan.

En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las posibles infracciones, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se

puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la ley.

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.

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.

En caso de comprobarse que la información facilitada o parte de ella no es veraz, se deberá suprimir en el momento en que se tenga constancia de dicha circunstancia, salvo que esa falta de veracidad sea intencionada y pueda constituir un delito, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

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 establecida en el artículo 32 de la LOPD-GDD.

Los empleados de la entidad y terceros externos deberán ser informados acerca del tratamiento de datos personales en el marco de los Sistemas de información a que se refiere el presente artículo.

10.5. Preservación de la identidad del informante y de las personas afectadas

El 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 del 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 del informante solo 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 en virtud de este apartado estarán sujetas las medidas de seguridad establecidas en la normativa aplicable. En particular, se le comunicará al informante antes de revelar su identidad, salvo que dicha comunicación pudiera comprometer la investigación o el procedimiento judicial. Cuando la autoridad competente se lo comunique al informante,

le remitirá un escrito explicando los motivos de la revelación de los datos confidenciales en cuestión.

11. INFORMACIÓN, FORMACIÓN Y MEJORA CONTINUA

La entidad se compromete a:

- 1) Informar de:
 - La existencia de los Canales Internos de Comunicación, presentes y futuros, creados con el fin de recibir informaciones.
 - El proceso para enviar dichas informaciones.
 - Los hechos denunciados a través del Sistema Interno de Información.
- 2) Promover y practicar una cultura de diálogo dentro de su estructura.
- 3) Participar activamente en las sesiones de formación del personal, especialmente para aquellas personas involucradas en la gestión de comunicaciones.
- 4) Mejorar continuamente el Sistema Interno de Información, teniendo en cuenta su idoneidad, adecuación y eficacia.

Cuando se determine la necesidad de modificar el Sistema Interno de Información, dicho cambio se llevará a cabo de manera planificada y se tendrá en consideración lo siguiente:

- a) El propósito de los cambios y sus posibles consecuencias.
- b) La integridad del Sistema Interno de Información.
- c) La disponibilidad de recursos.
- d) La asignación o reasignación de responsabilidades.
- e) El alcance y el plazo de implementación de los cambios.

La presente Política relativa al Sistema Interno de Información y la Defensa del Informante ha sido aprobada por la dirección de BOUTIQUE DEL SEGURO BALEAR CORREDURÍA DE SEGUROS, S.L., y entra en vigor desde la fecha de firma.

En Palma de Mallorca, a 30 de marzo de 2026

Firma por la entidad

Nancy Susana Platania
X4153000M