

Política del Sistema Interno de Información

1. INTRODUCCIÓN

Atocha S.A. de Seguros (en adelante, Seguros Atocha) se caracteriza por ser una entidad aseguradora consolidada y comprometida con la creación de valor, la mejora del crecimiento, rentabilidad y solvencia, respetando los principios y valores que se ven reflejados en nuestras acciones.

Por ello, tal y como se refleja en el Código de Conducta Empresarial, Seguros Atocha está comprometido con cumplir con sus compromisos, con mantener la integridad, el trato humano y la cercanía.

En los últimos años se han publicado varias normas que en unos casos aconsejan y en otros imponen la obligación de que las empresas cuenten con un canal interno de denuncias como medio de canalizar y facilitar la comunicación de infracciones de dicha normativa.

La Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, y su transposición a la legislación española por 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, aconsejan la integración de todos los canales de denuncias anteriormente referidos en un único canal interno de denuncias adaptado a la reciente normativa sobre protección de las personas informantes de forma que, sea cual sea la normativa en que se fundamente la denuncia, la persona informante quede amparada por las garantías de confidencialidad, anonimato y ausencia de represalias que la Ley 2/2023, de 20 de febrero, garantiza.

La utilización de LOS CANALES DE DENUNCIA INTERNA DE INFORMACIÓN serán el cauce preferente para realizar la denuncia; sin embargo, el denunciante tiene el derecho de elegir la vía más adecuada para tramitar su denuncia pudiendo optar por dirigirse a canales externos a la entidad, como la Autoridad Independiente de Protección del informante (A.A.I.) o las autoridades u órganos autonómicos correspondientes, así como, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

Este Canal de denuncias no podrá utilizarse para la realización de consultas concernientes a productos contratados o gestiones de siniestros, para lo que deberán dirigirse al Departamento correspondiente a las coberturas de su póliza o al Servicio de Atención al Cliente. Ni tampoco para realizar quejas o reclamaciones sobre el producto que tenga contratado o sobre la gestión de un siniestro, para lo que deberán dirigirse al Departamento de Quejas y Reclamaciones del Servicio de Atención al Cliente.

2. FINALIDAD

La Política del Sistema Interno de Información tiene como finalidad recoger los principales principios de funcionamiento y organización del sistema interno de información de Seguros Atocha, estableciendo un medio seguro por el cual las personas que tengan la condición de empleados, condición de autónomos, personas pertenecientes al órgano de administración, dirección o supervisión, que conforman Seguros Atocha, así como cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores, relacionados con Seguros Atocha, y las personas en el marco de una relación laboral o estatutaria ya finalizada, voluntarios, becarios, trabajadores en periodos de formación, así como 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, puedan comunicar las irregularidades que observen contrarias a los principios de conducta de la entidad o que constituyan actos ilícitos o infracción grave de la normativa administrativa, para que la empresa pueda adoptar las medidas correctoras y, en su caso, sancionadoras que considere pertinentes y, en todo caso, las medidas necesarias para la protección del informante y los afectados por el hecho denunciado.

ATOCHA S.A. DE SEGUROS, en cumplimiento de lo dispuesto 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, ha instaurado un SISTEMA INTERNO DE INFORMACIÓN, diseñado, establecido y gestionado de forma segura, de modo que se garantice la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, así como de las actuaciones que se desarrollen en la gestión y tramitación de la misma, impidiendo el acceso de personal no autorizado y adoptando las medidas procedentes para excluir todo acto de represalia contra la persona informante.

3. PRINCIPIOS

Los principios y valores por los que el funcionamiento del canal interno de Seguros Atocha se rige son:

- Integridad/Honestidad:

Cumplimos la legislación vigente y nos comprometemos a que todas nuestras actuaciones están regidas por los principios de honestidad e integridad, evitando y luchando contra cualquier tipo de corrupción e injusticia.

- Transparencia:

Es nuestro compromiso comunicarnos de manera clara, veraz, fiel y diligente en todos los ámbitos, tanto con nuestros empleados como con cualquier persona o entidad pública o privada vinculada a nuestra empresa.

- Transformación:

Generar cambios positivos en la sociedad es fundamental para nosotros. Mejorar nuestro entorno en el ámbito social, económico y ambiental son nuestras prioridades como compañía.

- Buena fe:

Las denuncias realizadas a través del canal interno de información deberán ser formuladas de buena fe, por lo que la información deberá ser veraz y precisa.

- Confidencialidad:

Seguros Atocha actuará garantizando la confidencialidad de la identidad del informante, y los afectados, así como la de los datos obtenidos durante el procedimiento de gestión de la información respecto de la que en todo caso se aplicará la normativa sobre Protección de Datos Personales.

Se limitará el acceso a los datos personales, que únicamente serán conocidos por el Responsable del Sistema.

En caso de que el Responsable del Sistema considere necesaria la intervención de terceros para llevar a cabo la fase de investigación deberá adoptar las medidas necesarias para garantizar que la información que les facilite no es utilizada a otros fines. Si considera necesaria la adopción de medidas disciplinarias podrá revelar la identidad del denunciado al responsable de RRHH y, en el caso de ser necesaria la adopción de medidas correctoras en la aplicación de la normativa, al responsable de los servicios jurídicos, debiendo dar cuenta en todos los supuestos anteriores al Delegado de Protección de Datos.

Así mismo podrán ser revelados los datos como consecuencia del requerimiento por parte de la Autoridad judicial, por la existencia de algún procedimiento judicial o administrativo.

- **Objetividad e Imparcialidad:**

Seguros Atocha actuará bajo los principios de objetividad e imparcialidad en el marco de sus actuaciones, al igual que el Responsable de gestión del tratamiento de la información recibida.

Las comunicaciones serán tratadas bajo las mismas pautas priorizando la igualdad de trato, y rechazando cualquier tipo de discriminación por motivo de nacimiento, raza o etnia, sexo, religión, discapacidad, o cualquier condición personal o social.

4. ESTRUCTURA

En cumplimiento de lo dispuesto 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, ATOCHA S.A. DE SEGUROS ha instaurado un SISTEMA INTERNO DE INFORMACIÓN, diseñado, establecido y gestionado de forma segura, de modo que se garantice la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, así como de las actuaciones que se desarrollen en la gestión y tramitación de la misma, impidiendo el acceso de personal no autorizado y adoptando las medidas procedentes para excluir todo acto de represalia contra la persona informante.

El SISTEMA INTERNO DE INFORMACIÓN ha sido dotado de un CANAL DE DENUNCIAS en el que han quedado integrados los distintos CANALES INTERNOS DE INFORMACIÓN que ATOCHA S.A. DE SEGUROS tiene establecidos e incorporará aquellos otros que en el futuro puedan implantarse, de forma que todos ellos queden amparados por las garantías que el SISTEMA INTERNO DE INFORMACIÓN brinda a las personas informantes.

El sistema de canal interno de información ha sido establecido y aprobado por el Órgano de gobierno de Seguros Atocha, y ha sido diseñado de modo que se garantice la confidencialidad de la identidad del informante y terceros afectados por la información desarrollando un procedimiento de gestión de las comunicaciones para su tratamiento.

La estructura del canal interno está encabezada por el Responsable del Sistema, que será nombrado por el órgano de gobierno y desarrollará sus actividades de forma independiente y autónoma respecto al resto de los órganos de la entidad, no pudiendo recibir instrucciones para el ejercicio de sus funciones, y se le proporcionarán todos los medios personales y materiales necesarios para llevarlas a cabo.

Tanto el nombramiento como el cese o destitución del Responsable del Sistema son competencia del órgano de administración de ATOCHA S.A. DE SEGUROS y se notificarán a la Autoridad Independiente de Protección del Informante o, en su caso, a las autoridades u órganos de las Comunidades Autónomas.

El Responsable de Gestión del Sistema se encarga de la tramitación de las denuncias, que serán registradas y posteriormente analizadas para su admisión o inadmisión.

Una vez decidida la admisión o inadmisión, el Responsable del Sistema abrirá la fase de investigación, donde se recabarán las pruebas y testimonios necesarios para emitir una resolución motivada.

Las comunicaciones a través del canal interno de información establecido en la plataforma web se podrán realizar de dos formas, por escrito o de forma verbal. Dicha plataforma web informará de forma clara y accesible sobre el procedimiento de gestión

de la denuncia y los derechos y garantías de denunciante y denunciado. En función de los hechos que quiera comunicar deberá elegir el CANAL INTERNO DE INFORMACIÓN que considere más adecuado al motivo de su denuncia de entre los que se ofrecen a continuación. Al hacer clic sobre el canal de denuncias elegido se abrirá un enlace informativo sobre los hechos que pueden ser denunciables a través del canal elegido. A continuación encontrarán dos formas de realizar la denuncia de los hechos, por escrito mediante un campo de texto o de forma verbal adjuntando un archivo en formato Mp3 o Mp4. Podrá seleccionar la opción que más le convenga. En ambos casos, podrá proporcionar los datos que considere pertinentes sobre los hechos objeto de la información, pudiendo hacerlo anónimamente, y adjuntar o proponer las pruebas que considere oportunas para su investigación. Se podrá, a solicitud del informante, presentar la denuncia mediante una reunión presencial, ya sea mediante una solicitud de petición de cita escrita o verbal. La reunión presencial deberá tener lugar en un plazo máximo de siete días desde su solicitud. El contenido de la reunión presencial se documentará mediante grabación de la conversación o a través de una transcripción completa y exacta. Recibida la comunicación será tratada desde la confidencialidad y bajo la normativa de protección de datos, garantizando la presunción de inocencia y honor de las personas intervinientes.

5. PROCESO DE GESTIÓN Y TRAMITACIÓN DE LA INFORMACIÓN ACUSE DE RECIBO Y REGISTRO:

Al enviar la información comienza el proceso de gestión y tramitación de la información, generando el sistema automáticamente un acuse de recibo en el que se indicará el número de expediente, y una dirección de correo electrónico a través de la cual el informante podrá comunicarse con el Responsable del Sistema de Información y/o para consultar el estado de la tramitación del procedimiento.

Seguidamente el Responsable del Sistema de Información procederá a su registro en el Libro Registro del Canal interno de información que corresponda, en el que se harán constar los siguientes datos:

- a) Fecha de recepción.
- b) Número de expediente.
- c). Actuaciones desarrolladas.
- d) Medidas adoptadas.
- e) Fecha de cierre.

ADMISIÓN O INADMISIÓN A TRÁMITE: Registrada la información, el Responsable del Sistema deberá comprobar si aquella expone hechos o conductas que se encuadren dentro del ámbito de aplicación de la protección que brinda el SISTEMA INTERNO DE INFORMACIÓN, decidiendo, en el plazo máximo de cinco días hábiles desde la fecha de entrada de la información, si la admite o inadmite a trámite.

La comunicación será inadmitida a trámite en cualquiera de los casos siguientes:

- a) Cuando los hechos relatados carezcan de toda verosimilitud.
- b) Cuando los hechos relatados no sean constitutivos de infracción normativa o administrativa grave o muy grave, infracción laboral, trato discriminatorio o ilícito penal.
- c) Cuando la comunicación carezca manifiestamente de fundamento o existan, a juicio del Responsable del Sistema, indicios racionales de haberse obtenido mediante la comisión de un delito. En este caso, además de la inadmisión, remitirá

al Ministerio Fiscal relación circunstanciada de los hechos que considere constitutivos de delito.

d) Cuando la comunicación no contenga información nueva y significativa sobre infracciones en comparación con una comunicación anterior respecto de la cual han concluido los correspondientes procedimientos, a menos que se den nuevas circunstancias de hecho o de Derecho que justifiquen un seguimiento distinto. En estos casos, el Responsable del Sistema notificará la inadmisión al informante de manera motivada.

La inadmisión se comunicará al informante dentro de los cinco días hábiles siguientes, mediante el correo electrónico canaldenuncias@segurosatocha.com, salvo que la comunicación fuera anónima o el informante hubiera renunciado a recibir comunicaciones.

Si la comunicación fuera admitida a trámite se comunicará al informante dentro de los cinco días hábiles siguientes, mediante el correo electrónico canaldenuncias@segurosatocha.com, salvo que la comunicación fuera anónima o el informante hubiera renunciado a recibir comunicaciones.

El Responsable del Sistema remitirá con carácter inmediato la información al Ministerio Fiscal cuando los hechos pudieran ser indiciariamente constitutivos de delito o a la Fiscalía Europea en el caso de que los hechos afecten a los intereses financieros de la Unión Europea, absteniéndose desde dicho momento de realizar cualquier gestión que pueda dificultar o poner en peligro la actuación de la Fiscalía.

INSTRUCCIÓN DEL EXPEDIENTE: La instrucción comprenderá todas aquellas actuaciones encaminadas a comprobar la verosimilitud de los hechos denunciados.

El Responsable del Sistema podrá solicitar al informante la ampliación o concreción de los hechos denunciados, mediante el correo electrónico canaldenuncias@segurosatocha.com, así como una relación de los medios de prueba que considere adecuados para la acreditación de los mismos y la aportación de las pruebas que obren en su poder si no las ha aportado con su denuncia, concediéndole al efecto un plazo de cinco días hábiles.

El Responsable del Sistema informará igualmente a la persona o personas afectadas por la información recibida, mediante el correo electrónico canaldenuncias@segurosatocha.com, dándoles traslado para que formulen alegaciones por escrito en el plazo de los siete días hábiles siguientes, acompañando una relación sucinta de los hechos que se les imputan e informándoles del tratamiento de sus datos personales. En ningún caso se comunicará a los sujetos afectados la identidad del informante ni se dará acceso a la denuncia.

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

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

El Responsable del Sistema interrogará personalmente a los testigos propuestos, en su caso, tanto por el informante como por la persona afectada.

TERMINACIÓN DEL EXPEDIENTE: Concluidas todas las actuaciones, el Responsable del Sistema emitirá un informe que contendrá, al menos:

- a) Una exposición de los hechos relatados junto con el código de identificación de la comunicación y su fecha de registro.
- b) La clasificación de la comunicación.
- c) Las actuaciones realizadas con el fin de comprobar la verosimilitud de los hechos.
- d) Las conclusiones alcanzadas en la instrucción y la valoración de las diligencias y de las pruebas e indicios que las sustentan.

Emitido el informe, el Responsable del Sistema adoptará alguna de las siguientes decisiones:

- a) Archivo del expediente, que será notificado al informante y, en su caso, a la persona afectada. En estos supuestos el informante tendrá derecho a la protección de su identidad, salvo que como consecuencia de las actuaciones llevadas a cabo en la fase de instrucción se concluyera que la información, a la vista de la información recabada, debía haber sido inadmitida.
- b) Remitir el informe al Ministerio Fiscal si, pese a no apreciar inicialmente indicios de que los hechos pudieran revestir el carácter de delito, así resultase del curso de la instrucción. Si el delito afectase a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.
- c) Trasladar el informe al Consejo de Administración de la entidad a fin de que por el mismo se adopten las medidas correctoras y/o sancionadoras que correspondan.

El plazo para finalizar las actuaciones y dar respuesta al informante, en su caso, no podrá ser superior a tres meses desde la entrada en registro de la información, salvo casos excepcionales que por su especial complejidad requieran una ampliación del plazo hasta un máximo de otros tres meses adicionales. La comunicación al informante se realizará mediante el correo electrónico canaldenuncias@segurosatocha.com.

6. PROTECCIÓN DE DATOS Y MEDIDAS DE DEFENSA DEL INFORMANTE

El tratamiento de datos personales por la entidad se regirá por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

No se recopilarán aquellos datos personales que no sean manifiestos para tratar una información específica, ni tampoco aquellos recopilados de forma accidental que serán eliminados sin dilación indebida.

Se entiende como lícito el tratamiento de datos personales necesarios en base a la disposición del artículo 6.1.c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y del artículo 8 de la Ley Orgánica 3/2018, de 5 de diciembre para cumplir con la aplicación de la obligación legal de creación de un Sistema interno de información impuesta por 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.

Cuando los datos personales se obtengan directamente del interesado se le facilitará la información prevista en la normativa legal del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre.

Se informa que en ningún caso se revelará la identidad del informante, quedando reservada por la entidad, a la persona o personas a las que se hace referencia en la comunicación ni a terceros.

Aquellos interesados podrán ejercer los derechos que se les otorga en virtud de los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

El acceso a los datos personales contenidos en el Sistema interno de información, quedarán reservados conforme a sus funciones y competencias a:

- a) El Responsable del Sistema.
- b) El órgano competente para la imposición de las oportunas medidas disciplinarias contra un trabajador.
- c) El responsable de los servicios jurídicos de la entidad para interponer si procediese las medidas legales necesarias en relación con los hechos de la información recibida.
- d) Los encargados del tratamiento de datos que se puedan designar.
- e) El delegado de la protección de datos de la entidad.

Será lícito el tratamiento de datos por terceros o la comunicación siempre que resulte necesario para imposición de medidas correctoras en la entidad, o si procediese para la tramitación de procedimientos sancionadores o penales.

Los datos que no sean objeto de tratamiento por no ser necesarios para la investigación de los hechos comunicados, y aquellos que se refieran a datos catalogados como especiales serán inmediatamente suprimidos.

Los datos que si son objeto de tratamiento por la entidad se conservarán en el sistema interno de informaciones durante el tiempo imprescindible para tomar la decisión de proceder o no a iniciar una investigación a raíz de los hechos comunicados. Si se acredita que la información no es veraz se procederá a su supresión, salvo que esa falta de veracidad constituya un ilícito penal, en cuyo caso se guardará para su uso en el marco de un procedimiento judicial. Los datos personales relativos a las informaciones recibidas y a las investigaciones internas en ningún caso podrán conservarse por un período superior a diez años.

Si no se hubiese iniciado ninguna investigación en el plazo de 3 meses desde que se tuvo recepción de la comunicación, se procederá a la supresión.

Se preservará la identidad del informante y de las personas afectadas o terceros mencionados. El Sistema interno de Información cuenta con las medidas técnico-organizativas pertinentes con el fin de protección y garantía de la confidencialidad de los datos obtenidos.

Únicamente se dará traslado de la identidad del informante cuando deba ser comunicada en el seno de una investigación penal, disciplinaria o sancionadora a la Autoridad Judicial, Ministerio Fiscal o autoridades administrativas correspondientes.

Las personas que hayan comunicado una de las infracciones previstas por la entidad tendrán derecho de protección siempre que se cumpla con dos determinadas condiciones:

La información debe haberse realizado conforme a los parámetros que marca la ley Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Se tenga suficientes indicios razonables para entender que la información a comunicar es veraz, aun cuando no se aporten pruebas determinantes, y siempre y cuando los hechos comunicados se encuentren dentro de uno de los ámbitos establecidos por la entidad para comunicar las infracciones.

Por tanto, se excluirá de protección a aquellas personas que comuniquen una información que ha sido analizada e inadmitida, informaciones que afecte a conflictos interpersonales, información pública o aquella fundada en rumores o informaciones que estén fuera del ámbito de aplicación del Sistema interno de Información.

Cualquier acto, amenaza o tentativa de represalia contra las personas que han presentado una comunicación y se encuentran bajo la protección anteriormente prevista está terminantemente prohibido.

Se considerará represalia todo aquel acto u omisión que esté prohibido por la normativa legal o el trato desfavorable en el contexto laboral o profesional hacia una persona por el hecho de su condición de informante situándole en una situación desventaja respecto al resto.

La entidad tomará medidas contra todo aquel que cometa represalias imponiendo las medidas disciplinarias que se determinen en cada caso.

Con el fin de la protección del informante la entidad garantiza que toda persona que realice una comunicación de las infracciones previstas no incurrirá en responsabilidad siempre y cuando dicha comunicación sea razonablemente fundada. Esta medida no se aplicará cuando existan responsabilidades de tipo penal.

En cuanto a la forma de adquisición o acceso que tuvo el informante de la comunicación, no se incurrirá en responsabilidad salvo que haya sido adquirido o se haya tenido acceso a este mediante la comisión de un delito.

Se informa que todo acto u omisión que no sea relacionado con la comunicación si será exigible en cuanto a su responsabilidad.

Para la protección de las personas afectadas por la comunicación se preservará en todo momento el derecho a la presunción de inocencia, el derecho a la defensa y el derecho al acceso al expediente, garantizando la confidencialidad de los datos e identidad del informante, y por último se protegerá su identidad y la confidencialidad de sus datos y del procedimiento.

La entidad podrá adoptar medidas disciplinarias bajo su potestad empresarial frente al personal laboral que se haya determinado que ha incurrido en alguna infracción de las previstas en virtud de la comunicación. Esta potestad podrá concurrir con la potestad sancionadora de la Autoridad Independiente de Protección del Informante y de los órganos competentes de las comunidades autónomas.

En todo lo no previsto en la presente Política del Sistema Interno de Información se aplicarán las disposiciones de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, y su transposición a la legislación española por 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.

CONTROL DE CAMBIOS

Versión	Modificaciones s/versión anterior	Fecha de Creación	Elaborado por	Revisado por	Fecha Revisión	Aprobado por Consejo de Administración
1.0	Creación del documento	mayo-23	Alejandro Jiménez Pinto.	Jaime de Sandoval González, Jasmín Senzano Fernandes, Alejandro Jiménez Pinto.	junio-23	nov-23
2.0	Revisión sin cambios			Alejandro Jiménez	sep-24	
3.0	Actualización plazos entrevista y conservación datos			Alejandro Jiménez	nov-24	