

PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES

Sistema Interno de Información



TABLA DE REVISIONES

Revisión	Descripción de la modificación	Fecha
00	Edición Inicial	26/02/2024

Elaborado por:
Responsable del Sistema

Revisado y Aprobado por:
Dirección

Firma:

Firma:

Contenido

1. Introducción y objetivo.....	3
2. Ámbito de aplicación	4
3. Identificación de los canales de información	7
3.1. Canal de Denuncias de AUTO ELECTROCHIPS	7
3.2. Otros canales de información.....	7
3.3. Canal externo de información	8
4. Gestión del Sistema Interno de Información.....	9
4.1. Fase de Registro.....	9
4.2. Fase de Análisis.....	10
4.3. Fase de Investigación.....	11
4.4. Fase de Resolución	12
5. Protección de datos personales	13
6. Medidas de protección.....	15
7. Actualización del Procedimiento	16

1. Introducción y objetivo

El 21 de febrero de 2023 se publicó en el Boletín Oficial del Estado 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. Con la aprobación de esta ley, se incorpora al Derecho español la Directiva (UE) 2019/1937 del Parlamento 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.

En cumplimiento de la Ley 2/2023, la Dirección de **AUTO ELECTROCHIPS, S.L.** (en adelante, **AUTO ELECTROCHIPS**) aprueba la **Política del Sistema Interno de Información** que tiene como objetivo definir los principios y premisas que regulan el Sistema Interno de Información, el cual se configura como una herramienta para fortalecer la cultura de la información/comunicación como mecanismo esencial para la prevención, detección y corrección de amenazas al interés público y de incumplimientos normativos, consolidar el marco de supervisión del riesgo de integridad y facilitar el cumplimiento de la normativa interna en particular.

Así mismo, la Dirección de **AUTO ELECTROCHIPS** aprueba el presente **Procedimiento de Gestión de Informaciones** cuya finalidad es establecer las previsiones necesarias para que el Sistema Interno de Información y los canales internos de información existentes cumplan con los requisitos establecidos en la Ley 2/2023.

2. Ámbito de aplicación

A través del Sistema Interno de Información de **AUTO ELECTROCHIPS** los empleados y agentes externos de la empresa pueden enviar mensajes para denunciar de buena fe:

- un delito, una violación manifiesta de las leyes aplicables o una amenaza o perjuicio del interés general; o
- violaciones manifiestas de las directrices internas, sus principios y sus políticas.

En el Sistema Interno de Información de **AUTO ELECTROCHIPS** los empleados y agentes externos de la empresa podrán enviar mensajes sobre los siguientes temas principales:

- **Corrupción y tráfico de influencias:**
 - Cualquier acto mediante el cual una persona solicite o acepte una ventaja indebida a cambio de realizar, acelerar la realización, dejar de realizar o demorar la realización de una acción durante sus deberes profesionales, para el beneficio de un tercero.
 - Ejemplos: Sobornos y aceptación sobornos; relaciones inadecuadas con autoridades públicas, proveedores o clientes; conflicto de intereses; tráfico de influencias; facilitación de pagos; etc.
- **Lavado de dinero / fraude/ falsificación de libros y registros:**
 - El lavado de dinero puede ocurrir cuando se realiza una acción en actividades económicas legítimas para enmascarar el verdadero origen de dinero o activos que están conectados con actividad criminal.
 - Ejemplos: Pagos hechos a o desde países que son «paraísos fiscales»; exceder los límites de pagos en efectivo; no cumplir con los requisitos de revelación; etc.
 - Fraude se refiere a la afirmación de falsedades o distorsión u ocultación de la verdad para obtener una ventaja ilegal para uno mismo o para un tercero.
 - Ejemplos: Fraude crediticio; fraude de subsidio; fraude de seguros; falsificación de documentos; información engañosa sobre un producto o sobre la venta; etc.
 - Falsificación de libros y registros se refiere a la malversación o justificación inadecuada de transacciones.
 - Ejemplos: Emitir facturas infladas para quedarse con el excedente; falta de documentación de respaldo; etc.
- **Apropiación de activos:**
 - Uso inadecuado de fondos corporativos, activos o información confidencial.
 - Ejemplos: Uso no autorizado de activos de la empresa para fines personales; robar bienes o equipos de la empresa; no devolver prendas de vestir o accesorios tomados prestados; uso no autorizado de secretos comerciales; etc.

- **Prácticas contra la libre competencia:**
 - Prácticas contra la libre competencia se refiere a actividades que restringen la competencia de manera ilegal.
 - Ejemplos: Acuerdos de precios; colusión en licitaciones; etc.
- **Violación de la protección de datos:**
 - Violaciones de las normativas destinadas a la protección de los datos personales; infracciones graves del secreto de las telecomunicaciones.
 - Ejemplos: Compartir sin autorización datos de clientes y empleados; abuso de datos para comunicaciones por correo electrónico y teléfono; etc.
- **Discriminación/ acoso y otros temas de RR.HH.:**
 - La discriminación se refiere a situaciones en las que una persona es tratada de manera diferente a las otras sin una razón legítima, en particular debido al color de la piel, sexo, religión, creencias políticas, origen nacional o social, edad, discapacidad, pertenencia a un sindicato, orientación sexual o identidad de género.
 - Ejemplos: Hostilidad debido a opiniones o creencias; xenofobia; discriminación en derechos de maternidad; etc.
 - Acoso, violencia o amenaza se refieren a cualquier forma de violencia u hostigamiento físico, sexual, verbal o psicológico, o amenaza del mismo tipo.
 - Ejemplos: Acoso sexual; humillación; conducta violenta; chantaje; etc.
- **Violaciones de las normas sociales y de la ley del trabajo/ y empleo ilegal:**
 - Las violaciones de las normas sociales y de la ley del trabajo se refieren a trabajo forzado o esclavo, tráfico de seres humanos, explotación infantil, restricción de la libertad de asociación y violaciones de las horas de trabajo.
 - Ejemplos: Empleo de niños menores de 16 años o de la edad que estipulen las leyes locales; retención de documentos de identidad; etc.
 - Empleo ilícito se refiere a actividades laborales que evaden el registro obligatorio y los requisitos de divulgación.
 - Ejemplos: Empleo de trabajadores indocumentados; omisión tributaria del pago; falta de registro del negocio; etc.
- **Violaciones de los reglamentos de salud y seguridad:**
 - Las violaciones de salud y seguridad se refieren a la falta de precauciones o instrucciones de seguridad, y a instancias de falta de cumplimiento con los reglamentos sobre salud y seguridad.

- Ejemplos: Falta de alertas ante fuentes de peligro; accidentes debido a medidas de seguridad insuficientes; condiciones de trabajo poco higiénicas o peligrosas; etc.
- **Violaciones de los reglamentos de protección medioambiental:**
 - Las violaciones de los reglamentos de protección medioambiental se refieren a la contaminación intencional o accidental del agua, el suelo o el aire.
 - Ejemplos: Derrame de sustancias peligrosas para el medioambiente; eliminación inadecuada de residuos; etc.
- **Violaciones de derechos humanos:**
 - Las violaciones de los derechos humanos se refieren a la negación o violación de los derechos consagrados en la Declaración Universal de los Derechos Humanos, siempre que no estén incluidos en alguno de los otros temas principales.
 - Ejemplos: Negación del derecho a la vida, la libertad y la seguridad; privación de bienes; sometimiento a trato degradante; negación del derecho a una remuneración justa y favorable, etc.

3. Identificación de los canales de información

El Sistema Interno de Información de **AUTO ELECTROCHIPS** integra los distintos canales internos de información afectados por la Ley 2/2023, lo que permite garantizar el cumplimiento de los estándares y garantías de gestión en todos ellos.

3.1. Canal de Denuncias de AUTO ELECTROCHIPS

El **Canal de Denuncias de AUTO ELECTROCHIPS** es la vía principal para informar sobre posibles irregularidades que puedan suponer infracciones que versen sobre actos o conductas, presentes o pasadas, referidas a los ámbitos de aplicación relacionados en la *Política del Sistema Interno de Información*.

Las comunicaciones pueden presentarse de forma nominativa, es decir, con identificación del interesado, o de forma anónima.

Este Canal permite la presentación de comunicaciones por escrito a través de:

- Plataforma corporativa accesible a través de: <https://canaldenuncias.electrochips.com/>
- Correo electrónico: sisinformacioninterna@electrochips.com
- Correo postal: **C/ Fidel Bautista Sánchez 22, Pol. Ind. Los Villares, 37184 Villares de la Reina (Salamanca)**

Las comunicaciones también pueden presentarse verbalmente mediante reunión presencial, a solicitud del interesado. En estos casos debe dirigirse la petición a través de alguna de las vías de comunicación escritas mencionadas anteriormente.

Estas reuniones, previo consentimiento del informante, serán documentadas a través de una transcripción completa y exacta de la conversación realizada. Se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

3.2. Otros canales de información

En la actividad diaria de **AUTO ELECTROCHIPS**, pueden realizarse comunicaciones por canales distintos a los anteriores o cuyo/s destinatario/s sean persona/s no responsables de su tratamiento, pero que por su temática deban incluirse en el alcance del Sistema Interno de Información.

En estos casos, el receptor debe instar al informante a utilizar el Canal de Denuncias y, en caso de no ser posible, estará obligado a remitir inmediatamente la comunicación al Responsable del Sistema de **AUTO ELECTROCHIPS** a través de la dirección de correo electrónico sisinformacioninterna@electrochips.com y garantizar la confidencialidad de la información recibida, tanto antes como después de su remisión al Responsable del Sistema, así como cumplir con el resto de las garantías y el marco de gestión establecido en el presente Procedimiento.

3.3. Canal externo de información

Sin perjuicio del acceso a los canales internos y en cualquier momento, toda persona física que forme parte de algunos de los colectivos con acceso al Sistema Interno de Información puede dirigirse a la Autoridad Independiente de Protección del Informante (A.A.I.) o ante las autoridades u órganos autonómicos correspondientes, para informar de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación de la Ley 2/2023.

En cualquier caso, el Responsable del Sistema, velará para la integración de este Procedimiento en la organización.

4. Gestión del Sistema Interno de Información

El Sistema Interno de Información de **AUTO ELECTROCHIPS** dispone de una serie de principios generales y garantías detallados en la **Política del Sistema Interno de Información**, y en base a ellos se define la gestión del Sistema Interno de Información.

El proceso de gestión incluye la participación de diferentes áreas para garantizar la preservación de la autonomía e independencia en todas las fases de la gestión de comunicaciones. Las gestiones se realizarán de forma personalizada y en colaboración con las partes implicadas, dejando constancia documental de todas las acciones realizadas.

El proceso de gestión del Sistema Interno de Información de **AUTO ELECTROCHIPS** incluye las siguientes fases:



4.1. Fase de Registro

Toda persona que forme parte de alguno de los colectivos con acceso al Sistema Interno de Información del **AUTO ELECTROCHIPS** podrá dirigir la comunicación a alguno de los canales internos anteriores, en cumplimiento del principio de la buena fe.

El informante deberá facilitar los datos que se estimen necesarios. En caso de optar por la plataforma del Canal de Denuncias, el interesado deberá enviar la comunicación cumplimentando el formulario de obtención de datos disponible. La plataforma es la misma para todas las categorías de infracción y está diseñada para guiar al usuario en los datos a introducir, señalando con un asterisco los campos de cumplimentación obligatoria.

Las comunicaciones pueden ser nominativas o anónimas y se registran en la plataforma. Para las nominativas, existe una opción para permitir notificaciones por email. En caso de aceptar dichas notificaciones, el informante recibirá una confirmación de envío y será avisado de las respuestas.

El informante puede optar por ampliar la información y documentación de la comunicación con posterioridad a su formulación, ya sea de manera voluntaria o por solicitud del Responsable del Sistema. Los nuevos hechos y documentación aportada serán considerados en el proceso de gestión.

En el caso de comunicaciones presentadas por otras vías distintas de la plataforma del Canal de Denuncias (correo electrónico, correo postal, reunión presencial), ya se trate de comunicaciones realizadas por el propio informante como aquellas remitidas al Responsable del Sistema por parte del canal o del receptor no responsable de la gestión, serán incorporadas al Canal de Denuncias una vez obtenida la información y documentación facilitada por el denunciante, de acuerdo con el presente procedimiento.

4.2. Fase de Análisis

Las comunicaciones presentadas serán objeto de un análisis de admisibilidad, quedando excluidas del alcance del Sistema Interno de Información las comunicaciones que:

- No queden comprendidas dentro del ámbito material de la Ley 2/2023 y/o que no versen sobre hechos/conductas sobre irregularidades que puedan suponer infracciones de la normativa interna de aplicación a **AUTO ELECTROCHIPS** según lo dispuesto en la Política del Sistema Interno de Información.
- Sean presentadas por un colectivo sin acceso al Sistema Interno de Información, como son los clientes.
- Hayan sido inadmitidas por algún canal interno de información.
- Versen sobre hechos disponibles para el público (información pública).
- Se encuentren vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación o revelación.
- Se fundamenten en meros rumores y/o no estén fundadas en sospechas o indicios concretos o determinados.
- Versen específicamente sobre el contenido de un fichero/documento no accesible para la organización y no aportado en la comunicación.
- Sean relativas a hechos/conductas que se encuentren en sede policial, administrativa inspectora y/o judicial.

No obstante, el Responsable del Sistema se reserva la potestad de admitir una comunicación que, a pesar de no cumplir los criterios de admisibilidad, concurra en ella un supuesto de hecho excepcional que requiera de gestión a través del Sistema Interno de Información.

Adicionalmente, es siempre recomendable que las comunicaciones estén soportadas por medio de pruebas documentales, siendo también admisibles las pruebas testificales (incluido el testimonio del propio informante) u otros medios de prueba admisibles en derecho, si bien su no aportación no supondrá por defecto su inadmisión.

El análisis de admisibilidad será realizado por el Responsable del Sistema, existiendo ciertas categorías definidas que requieren de un pre-análisis que está externalizado en un experto externo en aras de reforzar la independencia, la objetividad y el respeto a las garantías que ofrece el Sistema Interno de Información.

En el marco de la gestión de la comunicación, ya sea antes y/o después de su admisión, puede resultar necesario contactar con el informante para solicitar información adicional, aclarar algún aspecto o, incluso, realizar un acompañamiento. El formato utilizado para mantener contacto depende de las necesidades del caso y atendiendo el canal interno receptor de la comunicación.

Considerando las exclusiones de inadmisibilidad anteriores, el Responsable del Sistema comunicará al informante la decisión de admisión/inadmisión.

En caso de admisión, se iniciarán las diligencias de análisis a practicar, entre las que se encuentran la interacción con las partes interesadas y las comunicaciones y cumplimiento de los requisitos en materia de protección de datos personales. En caso de inadmisión, se finalizará la gestión del expediente y así se comunicará al informante.

Si la comunicación es admitida, se procede a su registro en la plataforma y se continúa con su gestión. Adicionalmente, se mantiene un registro histórico de las informaciones recibidas, que recogerá todas las gestiones realizadas y las investigaciones internas que hayan dado lugar, garantizando la confidencialidad de la información.

En caso de existir persona denunciada y/o afectada se comunica la recepción de la comunicación contra su persona y en paralelo se da traslado al equipo que vaya a realizar la investigación ([ver apartado 4.3.](#)).

Excepcionalmente, en aquellos casos en los que la comunicación realizada al denunciado y/o afectado podría poner en peligro el curso de la investigación de los hechos/conductas objeto de comunicación, podrá demorarse la comunicación, pero esta no podrá superar en ningún caso el plazo de 1 mes desde que se haya registrado.

En todo caso, la comunicación incluirá:

- la recepción misma de la comunicación y la fecha,
- las conductas/hechos que se atribuyen,
- el equipo responsable de su gestión, y
- el tratamiento que se realizará de sus datos de carácter personal.

La fase de análisis de la comunicación finaliza con la selección del equipo responsable de la investigación, sin perjuicio de que, según la especialidad de los hechos objeto de la comunicación deban intervenir otras áreas siempre que así se requiera para su resolución.

4.3. Fase de Investigación

Con independencia del origen de la comunicación, en función de la materia objeto de la comunicación, se mantendrá un contacto previo con el equipo de **AUTO ELECTROCHIPS** o, en su caso el equipo investigador oportuno, con el objetivo de tratar el objeto de la comunicación, siendo posteriormente remitida junto con toda la documentación disponible. Solamente se facilitará la identidad del informante:

- Si es un dato imprescindible para el curso de la investigación, y
- Siempre previo consentimiento del interesado.

La investigación se iniciará a la mayor celeridad posible.

La investigación se llevará a cabo de acuerdo con los procedimientos internos definidos, en cumplimiento de las garantías previstas en la **Política del Sistema Interno de Información** y, en cualquier caso, garantizando para todas las personas afectadas:

- El respeto a la presunción de inocencia y al honor, así como al derecho de defensa.
- El derecho a ser escuchadas en cualquier momento.
- El derecho a ser informadas de las acciones u omisiones que se le atribuyen. Adicionalmente, al traslado de la existencia de la comunicación al denunciado y/o afectado, si en el marco de la investigación realizada se detectase la participación en los hechos objeto de comunicación de personas no identificadas inicialmente en la comunicación, tanto por voluntad o desconocimiento del informante o aun identificándose a una persona denunciada se detecta que existen indicios de la

participación de otras personas al margen de la persona identificada como denunciada, con el objetivo de garantizar que todas las personas que puedan verse afectadas por una investigación interna derivada de una comunicación ostenten los mismos derechos, en el momento que se disponga de indicios razonables que relacionen de manera directa a una persona con los hechos objeto de comunicación, se procederá a realizar la comunicación oportuna a la persona o personas identificadas.

- La preservación de su identidad y la confidencialidad de los hechos y datos del procedimiento.

El procedimiento de investigación podrá incluir:

- Entrevistas personales con la fuente (informante) para recabar más información.
- Entrevistas personales con los departamentos y/o las personas involucradas de manera directa o indirecta en los hechos/conductas que potencialmente son irregulares, a criterio del equipo responsable de la investigación.
- Análisis de datos y obtención de información.
- Petición de pruebas periciales a profesionales internos o externos a **AUTO ELECTROCHIPS**.
- Otras diligencias de investigación o prueba que se consideren pertinentes y sean lo menos gravosas posibles con relación a la posición jurídica de la persona afectada.

El proceso de investigación quedará debidamente documentado, detallando los antecedentes, el objetivo, el alcance y las conclusiones alcanzadas.

Especialmente en el curso de la investigación, pero también con anterioridad a esta, podrá resultar necesario aplicar determinadas medidas de protección, tales como la eliminación de la coincidencia del lugar de trabajo o la gestión de incompatibilidades caso de que alguna de las personas implicadas en una comunicación tuviese relación de parentesco, afinidad o de consanguinidad con alguno de los intervinientes en su gestión, investigación o resolución.

4.4. Fase de Resolución

Considerando todos los elementos que constituyen la base para la formación de criterio, el Responsable del Sistema resolverá sobre el cumplimiento/incumplimiento de la normativa respecto los hechos/conductas objeto de comunicación, y así se comunicará a las partes involucradas a la mayor celeridad posible.

En caso de apreciarse incumplimiento por parte de una persona trabajadora, el Responsable del Sistema remitirá el expediente al departamento de Recursos Humanos, para la toma de las medidas oportunas. Si la propuesta de resolución contempla la adopción de medidas de otra naturaleza, el expediente se remitirá a la instancia competente que corresponda por razón de la materia o naturaleza de las medidas.

El plazo de resolución es de 3 meses desde la recepción de la comunicación; no obstante, si no pudiera obtenerse la resolución en el plazo indicado debido a circunstancias específicas del caso, en particular, la naturaleza y la complejidad del objeto de la comunicación, que puedan justificar que la investigación se demore, se informará a las partes involucradas y se continuará con su gestión hasta su efectiva resolución, aplicando en cualquier caso las medidas establecidas en la normativa de protección de datos. En cualquier caso, el plazo no podrá exceder de 6 meses.

5. Protección de datos personales

El Sistema Interno de Información de **AUTO ELECTROCHIPS** está diseñado, implementado y gestionado de forma segura, de modo que se garantiza la confidencialidad de las personas involucradas en las comunicaciones y de las actuaciones que se desarrollan en la gestión y tramitación de estas, así como de la protección de datos.

Los tratamientos de datos personales que deriven de la aplicación de la Ley 2/2023 se registrarán por lo dispuesto en el Título VI de esta ley y en la legislación aplicable en esta materia.

A los informantes se les informará 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. Así mismo, no se informará, en ningún caso, a la persona a la que se refieran los hechos relatados de la identidad del informante.

El acceso a los datos personales contenidos en el Sistema Interno de Información quedará limitado a las personas con potestad de gestión según las funciones que tienen asignadas, quedando expresamente prohibido divulgar cualquier tipo de información sobre las comunicaciones a personas no autorizadas. En cualquier caso, el acceso a estos datos quedará restringido, dentro del ámbito de sus competencias y funciones, exclusivamente a:

- El Responsable del Sistema.
- El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.
- El responsable de los servicios jurídicos de **AUTO ELECTROCHIPS**, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.
- Los encargados del tratamiento designados.
- Los delegados de protección de datos.

Será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

No se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una información específica o, si se recopilan por accidente, se eliminarán sin dilación indebida.

Los datos personales que sean objeto de tratamiento se conservarán en el Sistema Interno de Información únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados. Si se procede a la inadmisión de la comunicación por no cumplir con los criterios de admisibilidad definidos, se procederá a la supresión de los datos, salvo que la inadmisión se produjera por la falta de veracidad de la comunicación y ello pudiera constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

En todo caso, transcurridos 3 meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, se procederá a la supresión de los datos personales, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del Sistema Interno de Información. 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.

Los colectivos con acceso al Sistema Interno de Información serán informados acerca del tratamiento de datos personales.

6. Medidas de protección

Los informantes tendrán derecho a protección siempre que no concurra ninguna exclusión de las previstas en el apartado 3.2 del presente Procedimiento y siempre que concurren las circunstancias siguientes:

- Tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación, aun cuando no aporten pruebas concluyentes, y que la citada información entra dentro del alcance del Sistema Interno de Información.
- La comunicación se haya realizado conforme a los requerimientos previstos en la **Política del Sistema Interno de Información** y en el presente Procedimiento.
- Las personas que hayan comunicado información sobre acciones u omisiones de forma anónima pero que posteriormente hayan sido identificadas, tendrán también derecho a protección.

AUTO ELECTROCHIPS prohíbe expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación.

No se considerará que las personas que comuniquen información sobre acciones u omisiones en el alcance del Sistema Interno de Información o que hagan una revelación pública hayan infringido ninguna restricción de revelación de información, y aquellas no incurrirán en responsabilidad de ningún tipo en relación con dicha comunicación o revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública de dicha información era necesaria para revelar la acción u omisión.

Los informantes no incurrirán en responsabilidad respecto de la adquisición o el acceso a la información que es comunicada o revelada públicamente, siempre que dicha adquisición o acceso no constituya un delito.

Los informantes tendrán acceso a las medidas de apoyo establecidas por la Ley 2/2023.

7. Actualización del Procedimiento

El presente Procedimiento se someterá a revisión de Dirección con la misma periodicidad establecida para la **Política del Sistema Interno de Información**. No obstante, la Dirección de **AUTO ELECTROCHIPS**, como responsable del Procedimiento, revisará su contenido anualmente y, en caso de que lo estime pertinente, propondrá modificaciones que elevará para su aprobación por el Consejo de Administración.

Adicionalmente, la actualización del Procedimiento se podrá iniciar, en cualquier momento y a petición de cualquiera de los implicados en la gestión de informaciones que haya identificado la necesidad de su modificación, por:

- Cambios en el marco normativo.
- Cambios en los objetivos y estrategia de negocio.
- Cambios en el enfoque o procesos de gestión.
- Cambios derivados de los resultados obtenidos en las actividades de seguimiento y control.
- Nuevas políticas o modificaciones sobre las existentes que afecten al contenido de este Procedimiento.
- Modificación de la estructura organizativa que implique un cambio de funciones en la gestión de informaciones.