

PROTOCOLO SISTEMA INTERNO
DE INFORMACION SOCIETAT
MUNICIPAL D'APARCAMENTS I
PROJECTES

Versión	Fecha	Afecta a:	Breve descripción del cambio

PROTOCOLO DEL SISTEMA INTERNO DE INFORMACION

1. INTRODUCCIÓN

El Modelo de Prevención de Delitos existente en la Societat Municipal D'Aparcaments i Projectes (en adelante, SMAP, o la Organización) y los valores que ésta promueve requieren que los miembros de su órgano de administración y todos sus directivos, y empleados o personal (en adelante, el órgano de administración, los directivos y empleados de SMAP serán referidos conjuntamente como "Miembros de la Organización") actúen con integridad y asuman la responsabilidad de sus acciones cuando actúan en el marco de la actividad desarrollada por el SMAP.

El presente protocolo responde a la necesaria supervisión y seguimiento del << Modelo d' Organització i Gestió per la prevenció i detecció de delictes de la Societat Municipal d'Aparcaments i Projectes >> haciéndose necesario en este momento, la modificación del **punto 5 del Codi de Conducta de l'SMAP, referido al Canal de Denuncies**, de conformidad con los requisitos establecidos 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**.

Dicha normativa parte de la idea de la conveniencia de poner el foco de atención en la necesaria colaboración ciudadana para conseguir la eficacia del derecho y el buen funcionamiento de las instituciones públicas y privadas. Y, por ende, la necesidad de establecer instrumentos específicos para que, quienes conocen de actuaciones irregulares o ilegales, puedan facilitar estos datos con la tranquilidad y confianza de que se le brindarán todos los mecanismos de protección necesarios para que pueda seguir mostrando esta conducta valiente y de utilidad pública sin miedo a sufrir injerencias, presiones o represalias ni por parte de la persona a la que se acuse, o terceros vinculados a la misma, y/o de la propia organización.

A tales efectos, el SMAP, con la clara voluntad de atender y atajar en el seno de la propia organización, de forma diligente y eficaz, cualquier conducta irregular o ilegal susceptible de generar consecuencias perjudiciales para la misma, ha configurado un **Sistema Interno de Información** centrado en asegurar un uso asequible, con garantías de confidencialidad, de correcto seguimiento y tramitación de la información y de protección al informante a fin de erigirlo como el vehículo de información preferente.

En el desarrollo de este Sistema de Información, la organización ha considerado el cumplimiento de la normativa de protección de datos de España y de la Unión Europea.

2. OBJETO Y FINALIDAD

El Sistema Interno de información implementado por el SMAP, cumple el objeto de constituirse como el mecanismo idóneo a través del que informar, de

manera confidencial, las actividades y conductas potencialmente irregulares que se describirán en el apartado 3 del presente Protocolo.

Precisamente en aras a la efectividad de dicho Sistema Interno de información, se ha entendido como esencial el desarrollo de un protocolo, Protocolo del Sistema Interno de Información, que además de contener el detalle de cuál va a ser el modo en el que se tramitarán y gestionarán las informaciones recibidas, cumpla la finalidad de establecer un régimen óptimo de protección de las personas que hagan uso del Sistema interno de información, a fin de crear un clima de confianza que potencie su uso y ahonde en la cultura de integridad y confianza con la que nos identificamos, y que entendemos es fundamental para ayudarnos a prevenir y detectar amenazas tanto para el interés de la propia empresa como de la sociedad que nos rodea y con la que interactuamos diariamente en el desarrollo de nuestra actividad.

Así pues, y a modo de resumen, podemos asegurar que la finalidad del presente Protocolo es doble y se concreta en el establecimiento de:

- I. Un sistema interno de información, que abarca tanto el canal, entendido como el mecanismo o vehículo articulado para el envío y recepción de la información, como la identificación y desarrollo de la persona encargada del mismo, Responsable del Sistema.
- II. Un procedimiento de gestión de la información.
- III. Un sistema de protección dirigido a las personas que, en un contexto laboral o profesional, detecten infracciones penales o administrativas graves o muy graves y las comuniquen a través del canal implementado por el SMAP.

3. ÁMBITO PERSONAL Y MATERIAL DE APLICACIÓN

El Sistema Interno de Información implementado por el SMAP resulta de aplicación a cualquier persona que pretenda denunciar una posible infracción en el contexto profesional del SMAP, concretamente a todas aquellas personas que, como consecuencia de su relación directa o indirecta con la organización, y en un contexto laboral o profesional, hayan obtenido información sobre infracciones, comprendiendo en todo caso a:

- Los empleados que mantienen relación con el SMAP.
- Los profesionales, colaboradores de la organización, con independencia del nivel jerárquico y la posición que ocupan dentro de la organización.
- Las personas que ejercen las responsabilidades más altas de la organización.
- El equipo directivo.
- Aquellas que aunque no sean empleados, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección.

- Los representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante.

Y se estable como un canal confidencial a través del cual poder trasladar posibles conductas irregulares o ilícitas de las que puedan haber sido testigos, o tengan conocimiento, y que estén relacionadas con:

- Infracciones del Derecho de la Unión Europea siempre que:
 - i) Se enmarquen en el ámbito de la contratación pública (salvo procedimientos que hayan sido declarados secretos o reservados), adjudicación de concesiones o contratos, servicios, productos y mercados financieros, prevención del blanqueo de capitales y financiación del terrorismo, mercado y consumidores, medio ambiente, naturaleza, biodiversidad y clima, así como salud pública y protección y bienestar de los animales.
 - ii) Afecten a intereses financieros de la Unión Europea,
 - iii) Incidan en el mercado interior y/o
 - iv) Se cometan en materia de competencia, ayudas otorgadas por el Estado, o fiscalidad.
- Acciones u omisiones que puedan ser constitutivas de infracción penal.
- Acciones u omisiones que puedan ser constitutivas de infracción administrativa, siempre que tengan la consideración de grave o muy grave.
- Infracciones penales o administrativas graves o muy graves que impliquen quebranto económico para la Hacienda Pública y la Seguridad Social.
- Infracciones del derecho laboral en materia de seguridad y salud en el trabajo, ello sin perjuicio de la regulación establecida en su normativa específica.
- Incumplimientos de normas, protocolos, procedimientos o políticas internos de la Empresa, o de la legislación vigente y aplicable.

Las comunicaciones que se realicen a través del Sistema Interno de Información se referirán, exclusivamente, a conductas que pudieran efectivamente afectar de forma razonable a la relación laboral o profesional entre la organización y sus empleados, colaboradores y, nunca referidas a ámbitos vinculados a la vida privada de las personas.

Los Informantes sólo deberán proporcionar aquella información específica y objetiva que sea necesaria para determinar si el objeto de su comunicación se

encuentra dentro del alcance para el que se implementa el Sistema Interno de Información.

Asimismo, deberán evitar, salvo que sea indispensable para entender el alcance de la información, facilitar datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, así como datos biométricos, datos relativos a la salud o datos relativos a la vida sexual u orientaciones sexuales del informador, persona denunciada o cualesquiera otra persona física relacionada o vinculada a los hechos comunicados a través del sistema interno.

El Sistema Interno de Información a que se refiere el presente protocolo, complementa, pero NO sustituye los canales de comunicación que la organización ya tiene desarrollados para materias específicas, como son p.ej. de acoso laboral. En definitiva, el Sistema Interno de Información se erige como un mecanismo más a disposición de los Informantes, sin perjuicio de que siguen teniendo abierto el cauce normal de comunicación a través de sus superiores jerárquicos.

4. SISTEMA INTERNO DE INFORMACIÓN

El Sistema Interno de Información implementado se erige como el cauce preferente para informar sobre las acciones u omisiones previstas en el apartado anterior, siempre que se pueda tratar de manera efectiva la infracción y no exista un riesgo real de represalia para el denunciante.

A efectos de evitar lo anterior, el referido Sistema cumple con los siguientes requisitos y estándares: i) Permitir a todas las personas referidas en el apartado 3, comunicar información sobre las infracciones previstas en dicho apartado. ii) Estar diseñado, establecido y gestionado de una forma segura, de modo que se garantice la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la protección de datos, impidiendo el acceso de personal no autorizado. iii) Permitir la presentación de comunicaciones por escrito o verbalmente, o de ambos modos. iv) Integrar los distintos canales internos de información que pudieran establecerse dentro de la organización. v) Garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva, con el objetivo de que el primero en conocer la posible irregularidad sea la propia organización. vi) designar a un Responsable del Sistema. vii) desarrollar una política o estrategia que enuncie los principios generales en materia de Sistema interno de información y defensa del informante y que sea debidamente publicitada en el seno de la organización. viii) contar con un procedimiento de gestión de las informaciones recibidas. ix) establecer las garantías para la protección de los informantes en el ámbito de la propia organización.

5. CANALES QUE INTEGRAN EL SISTEMA INTERNO DE INFORMACIÓN

Los Informantes podrán realizar comunicaciones por escrito o verbalmente a través de los siguientes medios o canales:

- Por escrito, a través de correo postal o cualquier medio electrónico habilitado, concretamente a través de un formulario de denuncia incluido en la página web. En cuyo caso se generará de forma instantánea un código de seguimiento único y personal para cada Informador, que le permitirá hacer un seguimiento del estado en el que se encuentra la tramitación de su Comunicación. Se anexa enlace de acceso directo al mismo

<https://www.mobipalma.mobi/es/mobilitat/estacionament/aparcamentssmap/>

- Verbalmente, por vía telefónica a través del número 971 214646 o través de sistema de mensajería de voz.
- A solicitud del informante, también podrá presentarse mediante una reunión presencial en el despacho del Responsable del Sistema o lugar expresamente convenido entre las partes. Este encuentro deberá celebrarse, con carácter general, en el plazo máximo de siete días a aquel en el que se hubiese solicitado la audiencia.

De formalizarse la comunicación por cualquiera de los dos últimos cauces habilitados, esto es por un medio verbal, el responsable del Sistema documentará la conversación: i) mediante una grabación, siempre que haya sido autorizado por el informante, en un formato seguro, duradero y accesible o ii) a través de una transcripción completa y exacta de la conversación.

Sin perjuicio de los derechos que le corresponden de acuerdo con la normativa sobre protección de datos, se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

De este modo, y para ahondar en la implementación de un clima de confianza que propicie el uso de los canales habilitados por parte de quienes fuesen conocedores de circunstancias que debieran ser comunicadas a la organización en cumplimiento del presente Protocolo, se permite de forma expresa la comunicación efectuada de manera anónima.

6. RESPONSABLE DE LA GESTIÓN DEL SISTEMA

El Comité Compliance, como responsable de la implementación del Sistema, es también el competente para la designación de la persona física responsable de la gestión de dicho sistema, en adelante el «Responsable del Sistema», así como de su destitución o cese.

Siendo que fue aprobado en el acta de la sesión nº 4/2022 del Comité de Compliance que será la Unitat de Seguiment de Risco Penals del SMAP la encargada de la tramitación de las denuncias, así como la composición de la misma, al amparo de lo dispuesto en el artículo 8.2 de la Ley 2/2023 reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, se ha optado por delegar a uno de sus

miembros, las facultades de gestión del Sistema Interno de Información, en adelante Responsable del Sistema, coincidente con quien ocupa el cargo de Cap d'Àrea de RRHH i Jurídic.

El Responsable del Sistema asume las siguientes labores:

- Recepción, verificación y tratamiento de las comunicaciones recibidas.
- Gestión y mantenimiento del archivo de los casos recibidos y de los expedientes generados.
- Revisión y control del funcionamiento del Sistema Interno de Información.
- Elaboración de un informe anual de la gestión del Sistema Interno de Información y traslado del mismo al Órgano de Administración del SMAP, para su inclusión en el informe anual de seguimiento del Modelo de Prevención de delitos.
- Actualización periódica del Protocolo del Sistema Interno de Información.

El Responsable del Sistema, así como, en su apoyo, las personas que hayan actuado por su designación, y cualquier persona que intervenga en las fases de gestión y tramitación del Sistema Interno de Información o en la tramitación de comunicaciones, deberán actuar con respeto a lo establecido en el presente Protocolo, realizando el trabajo con la máxima diligencia y confidencialidad, absteniéndose de revelar informaciones, datos o antecedentes a los que tengan acceso en el ejercicio de su tarea, así como de utilizarlos en beneficio propio o de un Tercero.

De igual modo habrán de abstenerse de actuar en aquellos supuestos en los que, por las personas a que afecta la información o de la materia que se trata, se deriva conflicto de interés, comunicándolo de forma inmediata, a la Unitat de Seguiments de Riscos Penals o, en su defecto, al órgano de administración, quien será el encargado de asignar la tramitación de la denuncia formulada a una persona cualificada en la que no concurra dicha situación. Este nuevo nombramiento será, en su caso, comunicado al informante a través del canal que hubiese facilitado a efectos de notificaciones.

El Responsable del Sistema deberá desarrollar sus funciones de forma independiente y autónoma del resto de órganos y/o departamentos del SMAP. No podrá recibir instrucciones de ningún tipo en su ejercicio, y deberá disponer de todos los medios personales y materiales necesarios para llevarlas a cabo.

7. PRINCIPIOS REGULADORES DEL SISTEMA INTERNO, GARANTÍAS Y MEDIDAS DE PROTECCIÓN

▪ **Obligación de comunicar**

Los miembros del SMAP, así como terceras partes vinculadas a la organización, que tuvieran indicios racionales y razonables de la comisión de una irregularidad o de algún acto contrario a la legalidad, o a las normas

internas aplicables que la Organización adopte voluntariamente, deberán comunicarlo al Responsable del Sistema a través de los canales habilitados.

Todos los empleados tienen la obligación de poner en conocimiento del Responsable del Sistema cualquier dato o indicio de que pueda haberse cometido o pueda cometerse un incumplimiento o infracción.

▪ **Otorgamiento de medidas de protección y de apoyo**

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.

El informador que haga uso del Sistema Interno de Información tiene derecho a que su identidad no sea revelada a terceras personas y a protección siempre que concurren las siguientes circunstancias:

a) tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación o revelación, aun cuando no aporten pruebas concluyentes, y que la citada información entra dentro del ámbito de aplicación de esta ley,

b) la comunicación o revelación se haya realizado conforme a los requerimientos previstos en esta ley.

De este modo, quedarán expresamente excluidas de toda medida de protección los informantes que hayan comunicado o revelado:

a) Informaciones 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,

b) Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores, e

c) Informaciones que se refieran a acciones u omisiones no comprendidas en el ámbito de aplicación definido en el apartado tercero del presente Protocolo.

La valoración de esta circunstancia se llevará a cabo por el Responsable del Sistema en la fase de recepción y análisis preliminar de la comunicación. Sin perjuicio de que la situación pueda ser objeto de nueva revisión durante la fase de investigación si existe una modificación de las circunstancias que provocaron la inaplicación de las medidas en la fase previa.

Del mismo modo, las personas que comuniquen o revelen infracciones conforme a lo previsto en el presente Protocolo contarán con el apoyo del Responsable del Sistema, quien les informará y asesorará de los procedimientos y recursos disponibles, de la protección frente a las represalias y de los derechos que le asisten.

La persona que haya comunicado o revelado información de forma anónima, pero cuyos datos hayan sido conocidos con posterioridad, tendrá igualmente derecho a que le otorguen medidas de protección y apoyo.

▪ **Confidencialidad**

Quien presente una comunicación a través del Sistema Interno de Información tiene derecho a que su identidad no sea revelada a terceras personas, por ello el SMAP garantizará la máxima confidencialidad de las comunicaciones recibidas, así como de la identidad del Informador, que no se revelará al denunciado ni al resto de la organización sin su consentimiento.

Todas las personas que, siempre que sea estrictamente necesario para la adecuada gestión de la Comunicación, tengan conocimiento de esta, estarán obligadas a mantener rigurosa confidencialidad de las Comunicaciones en todos sus extremos, incluyendo los datos de las partes intervinientes en el proceso, en especial acerca de la identidad del informador.

Dicha obligación de confidencialidad quebrará, únicamente, en aquellos supuestos en los que el Responsable del Sistema se vea obligado a revelar y/o poner a disposición información y/o documentación relativa a sus actuaciones, incluida la identidad de las partes implicadas, a requerimiento de la autoridad judicial o administrativa competente.

▪ **Prohibición de represalias, garantía de indemnidad y presunción de inocencia**

Queda estrictamente prohibido los actos constitutivos de represalias, incluidas las tentativas y amenazas de represalia, contra cualquier persona que, de buena fe, ponga en conocimiento, a través del Sistema Interno de Información, incumplimientos de la normativa interna, así como contra aquellos que puedan colaborar en la investigación o ayuden a resolverla.

Si el Responsable del Sistema confirmara que algún Interesado que hubiera actuado de buena fe, ha sido objeto de alguna medida sancionadora o represalia, los autores o responsables de estas serán objeto de investigación y, en su caso, les será aplicada las medidas disciplinarias correspondientes.

A estos efectos se entenderá por represalia cualesquiera actos u omisiones que estén prohibidos por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, solo por su condición de informantes, o por haber realizado una revelación pública.

SMAP garantizará la protección adecuada de la intimidad y de los datos personales y la preservación del honor, la presunción de inocencia y el derecho a la defensa de los Denunciados o personas afectadas por la comunicación, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento y, muy en especial en los supuestos de Comunicaciones infundadas, falsas o de mala fe, frente a las que se adoptarán, en su caso, las medidas disciplinarias que correspondan.

En el ejercicio del derecho de defensa el denunciado podrá solicitar expresamente la intervención de los representantes de los trabajadores y hacer valer cuantas pruebas considere oportunas.

▪ **Medidas de protección frente a represalias**

A efectos de asegurar una adecuada protección del informante y de evitar que frente al mismo puedan llegar a activarse represalias o a derivarse responsabilidades por la información facilitada en relación a una conducta irregular o ilícita comunicada a través del sistema interno de información, el SMAP ha decidido adoptar las siguientes medidas de protección:

- No considerar que quienes informen o hagan relevaciones públicas de acciones y omisiones recogidas en el apartado tercero del presente Protocolo hayan infringido ninguna restricción de revelación de información y, por lo tanto, dejarlas indemnes de cualquier responsabilidad por esta circunstancia.

- No exigir responsabilidad por el modo en el que se ha adquirido o se ha tenido acceso a la información que es comunicada o revelada públicamente, siempre que dicha adquisición o acceso no constituya un delito.

No obstante lo anterior, sí que será posible exigir responsabilidad a los informantes, o a cualquiera de las personas anteriormente referidas, por los actos u omisiones que no estén relacionados con la comunicación o la concreta revelación pública efectuada.

▪ **Derecho a ser oído y de acceso al expediente.**

De conformidad con las previsiones del apartado 8 del presente Protocolo, en el transcurso de la investigación de la Comunicación, la organización garantizará el derecho de acceso al expediente y de audiencia del Informador y del Denunciado, quienes, en su caso, podrán ejercer su defensa y plantear los argumentos, alegaciones y pruebas que a su derecho convengan en la fase de investigación de la Comunicación y ante el instructor designado.

▪ **Denuncias falsas**

Se entenderá como denuncia falsa: (i) aquella que no esté basada en hechos o indicios de los que razonablemente pueda desprenderse un hecho anómalo o comportamiento irregular; (ii) la formulada aun cuando el autor sea consciente de la falsedad de los hechos y/o los tergiversar voluntariamente.

En el caso de que, como resultado de la investigación se compruebe que una denuncia ha sido interpuesta de mala fe en base a datos falsos o tergiversados, se comprobará si existe relación laboral con el informador para, en su caso, adoptar las medidas disciplinarias que resulten precedentes al amparo del Convenio Colectivo aplicable y normativa interna.

▪ **Transparencia en relación con el uso de datos personales.**

La organización garantiza la aplicación del principio de transparencia en relación con el uso de los datos personales en el Sistema Interno de Información.

8. PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES

8.1. Recepción, análisis preliminar y admisión de las Informaciones

Las informaciones realizadas a través del Sistema Interno de Informaciones serán recibidas y registradas por el Responsable del Sistema, asignándoles un código único de identificación.

Al presentar la información, el informante podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones, pudiendo asimismo renunciar expresamente a la recepción de cualquier comunicación de actuaciones llevadas a cabo como consecuencia de la información.

Una vez recibida la información y, constatado por el Responsable del Sistema que nos encontramos ante un posible incumplimiento que recaiga dentro del ámbito de aplicación del presente Sistema, la misma pasará a tener el tratamiento de denuncia y se someterá a un análisis preliminar al objeto de determinar su aceptación e investigación o, en su caso, su rechazo.

El Responsable del Sistema documentará los motivos para admitir a trámite y registrar o para rechazar una comunicación relativa a un posible incumplimiento, a través de una ficha, que podrá contener, según los casos, la siguiente información:

- Denominación descriptiva de la denuncia, con expresión de su número de referencia única y su fecha de recepción.
- Resumen de datos aportados en la denuncia, con la discriminación de los datos objetivos y los datos subjetivos.
- Análisis de la información y la documentación remitida con la denuncia.
- Valoración del contenido de la denuncia y de la fiabilidad del informador.
- Decisión sobre la admisión a trámite de la denuncia, con expresión, si se considera oportuno, de las actuaciones a seguir.
- Designación del instructor responsable, si se valorase conveniente delegar esta función, por parte del Responsable del Sistema.

En este análisis preliminar se valorará la conveniencia de remitir a otras áreas de la organización afectada por la información aquellas comunicaciones que no sean objeto de este Sistema Interno de y/o que tengan un procedimiento distinto y específico regulado en el seno de esta, de lo que se dará traslado al informante.

El órgano que fuese competente para atender la misma deberá informar al Responsable del Sistema de la tramitación que se ha dado a la comunicación para éste lo pueda incluir en su informe anual.

También se decidirá si procede acumular la instrucción a otros procedimientos análogos ya en curso.

Una vez realizado el análisis preliminar, el Responsable del Sistema procederá, en la medida de lo posible, y dentro del plazo máximo de siete días a contar desde aquel en el que hubiese recibido la comunicación, a:

- Si la denuncia es considerada no pertinente, improcedente, carente de toda verosimilitud, o no relacionada con los fines del presente Protocolo, enviar al informador una notificación informativa de ello.
- Comunicar el traslado de la denuncia al canal específico que existiese dentro de la organización para la gestión de conductas vinculadas con áreas concretas como, por ejemplo, de acoso laboral.
- Cuando la denuncia sea considerada como pertinente, pero su contenido sea insuficiente, incompleto, o no proporcione el detalle necesario para que se pueda iniciar la instrucción del expediente, entonces se remitirá una notificación trasladando al informador la aceptación de la comunicación y solicitando la información adicional necesaria.
- Cuando la denuncia sea pertinente, y la información o documentación facilitada sea suficiente para el inicio de la correspondiente instrucción del expediente, entonces se remitirá una notificación informando al informador sobre el inicio de la gestión de la correspondiente instrucción

8.2. Apertura de la fase de investigación

Si, tras el análisis de los hechos contenidos en la Comunicación, el Responsable del Sistema considera que concurren en el caso indicios razonables de la existencia de incumplimientos. En este caso, y en función de la naturaleza del asunto, podrá recabar la asistencia de departamentos o instructores específicos, comunicándose la identidad de los mismos al Informador.

Estos instructores deberán guardar confidencialidad y secreto profesional en su intervención y respetar en todo caso los principios de este Protocolo.

Paralelamente a la apertura del expediente y a la incoación de la investigación, el Responsable del Sistema, podrá adoptar las medidas adicionales urgentes, a fin de evitar poner en riesgo el desarrollo de la investigación o que sean precisas para proteger al informador. Para poder llevar a cabo dichas acciones, el Responsable del Sistema se apoyará en los departamentos o áreas funcionales que correspondan.

La apertura del expediente también podrá hacerse de oficio por el Responsable del Sistema cuando haya tenido conocimiento por sí mismo de la posible infracción o incumplimiento.

8.3. Investigación interna de la comunicación

En el desarrollo de la investigación interna, el Responsable del Sistema, así como los terceros específicamente designados que, en su caso, participen o colaboren en la investigación, habrán de poner de manifiesto al denunciado el contenido de la denuncia que le afecte, dando la oportunidad de exponer y acreditar su posición respecto de su contenido. La instrucción se desarrollará en función del tipo de denuncia y de las comprobaciones que resulten precisas. En el transcurso de la instrucción se podrán realizar las siguientes actuaciones:

- Solicitud de aclaración/información adicional: en los casos que se precise, requerirá al informador para que la aclare o complemente, aportando los documentos y/o datos de que pudiera disponer para acreditar la existencia de la actuación o conducta irregular.
- Comprobación de la veracidad y la exactitud de la comunicación en relación con la conducta descrita, respetando los derechos de los afectados. Todos los miembros de la organización están obligados a colaborar lealmente durante el proceso de verificación. Las intervenciones de testigos y afectados tendrán carácter estrictamente confidencial. Podrán solicitarse notas o informes a Departamentos o Áreas afectadas.
- Entrevista con el denunciado: respetando sus derechos, se le informará del contenido de la comunicación para que exponga su versión de lo sucedido y pueda aportar los medios de prueba de los que dispusiere. Así mismo se mantendrán entrevistas privadas con todas las personas que pudieran verse involucradas. En todo caso se levantará acta por escrito de estas, que deberá firmarse por los intervinientes al término de las reuniones.
- Atendiendo a la naturaleza de los hechos investigados, las entrevistas podrán realizarse con la presencia de un testigo (superior jerárquico, compañero de equipo u otra persona que se estime conveniente). En este caso, el testigo también habrá de firmar las actas de las reuniones.
- Informes periciales de profesionales internos o externos.
- Acceso a documentos relacionados con el hecho denunciado, incluso a correos corporativos del denunciado, conforme las normas establecidas para ello.
- Otras actuaciones que se estimen necesarias durante la tramitación.

Se dejará constancia de todas las sesiones y entrevistas realizadas en el transcurso de la instrucción. En el caso de reuniones formales, en el momento de la finalización de cada reunión, se firmará una nota resumen con la conformidad, en lo posible, de todos los presentes.

Si la Comunicación implica directa o indirectamente al Responsable del Sistema y/o a alguno de los responsables designados para colaborar en la investigación, estos deberán abstenerse de participar en la investigación y resolución de la misma, pasando la competencia para la gestión de la denuncia a la Unitat de seguiment de Riscos Penals.

El SMAP se reserva expresamente el derecho de adoptar las medidas de vigilancia y control necesarias sobre las herramientas y medios informáticos que la organización pone a disposición de sus empleados, incluyendo el contenido de las comunicaciones y dispositivos, respetando, en todo caso, la legislación vigente sobre la materia y garantizado el principio de proporcionalidad y la dignidad del empleado.

8.4. Información y trámite de audiencia

Las personas cuyas conductas hubieran sido denunciadas e identificadas como presuntamente irregulares en la Empresa, serán informadas por Responsable del Sistema o investigador designado, de esta circunstancia así como del tratamiento de sus datos, tan pronto como la situación del procedimiento lo permita y, en cualquier caso, en el plazo máximo de un (1) mes, desde la recepción de la Comunicación, siempre que ello no obstaculice la correcta investigación de los hechos comunicados. El citado plazo podrá ser ampliado de manera motivada cuando se aprecien razones que así lo aconsejen.

Además, a través del trámite de audiencia, el instructor garantizará el derecho del Interesado y del Denunciado a plantear por escrito los argumentos, alegaciones y pruebas que a su derecho convengan.

8.5. Conclusiones y resolución de la investigación

Con base en las conclusiones alcanzadas durante la investigación interna se elaborará un informe y una conclusión o resolución. Si hubiese intervenido un instructor, éste presentará un informe firmado con su propuesta de resolución, que habrá de ser ratificada igualmente con la firma del Responsable del Sistema.

El escrito de resolución deberá contener, como mínimo, los siguientes extremos:

- Breve descripción de la investigación
- Hechos probados por la investigación y actuaciones desarrolladas
- Valoración o calificación de los hechos probados

- Conclusiones, que podrán comprender, según el caso:
 - Resolución del incumplimiento, que deberá incluir la adopción de las siguientes medidas: i) La corrección inmediata del incumplimiento y la adopción de las medidas de reparación del derecho vulnerado y de prevención de futuros incumplimientos que, en su caso, correspondan., ii) La sanción y/o medidas disciplinarias, que podrán ir desde el simple apercibimiento o amonestación, hasta el despido, iii) si las actuaciones comprobadas tuvieran relación con una actuación administrativa o judicial, sea parte o no la Organización, se informará de inmediato a la Asesoría Jurídica y a las autoridades competentes.
 - El archivo del caso, en el supuesto de que se concluya que no ha existido incumplimiento alguno.

Como garantía del procedimiento, únicamente se comunicará el contenido de la resolución y el tipo de medidas que, en su caso, se establezcan, al responsable del departamento o área correspondiente y a los Interesados y Denunciados, para la planificación y ejecución de estas.

En cualquier caso, las conclusiones serán puestas en conocimiento al Comité de Cumplimiento Penal, de forma que será este quien haga efectiva la medida que se hubiese acordado después de la investigación.

El procedimiento deberá completarse en el plazo más breve posible, no superando los tres meses, salvo que la naturaleza de la materia investigada así lo requiriese, en cuyo caso podría prorrogarse dicho plazo inicial por igual término de tres meses.

8.6. Cierre del expediente y elaboración de informes de reporte

En todo caso, de las comunicaciones recibidas, calificación y resolución se creará un registro sin datos personales, para acometer los estudios e informes correspondientes, y promover la corrección de las situaciones en que proceda.

De las comunicaciones recibidas, su gestión y, en su caso, resolución, el Responsable del Sistema dará cuenta periódicamente al Comité de Cumplimiento Penal, elaborando igualmente al final del año un informe en el que se relacionarán todas las comunicaciones recibidas y características de las mismas.

8.7. Registro de informaciones

Todas las informaciones que se comuniquen a través de los canales que integran el Sistema de Información, quedarán debidamente reflejadas en el “Libro-Registro de Comunicaciones” habilitado por la organización, siendo el garante de su cumplimiento y custodia el propio Responsable del Sistema.

El Libro-Registro de Comunicaciones no es público, por lo que únicamente a petición razonada de la Autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquella, podrá accederse total o parcialmente a su contenido.

9. SUPUESTOS DE EXENCIÓN Y ATENUACIÓN DE LA SANCIÓN

En los supuestos en los que la persona que hubiese participado en la comisión de la infracción administrativa objeto de la información sea la que comunique su existencia con anterioridad a que le hubiera sido notificada por parte de la organización la incoación del procedimiento de investigación como consecuencia de la información recibida por otro informante, el Responsable del Sistema podrá eximirle del cumplimiento de la sanción que le correspondiera siempre que resulten acreditados en el expediente los siguientes extremos:

- a) Haber cesado en la comisión de la infracción en el momento de presentación de la comunicación o revelación e identificado, en su caso, al resto de las personas que hayan participado o favorecido aquella.
- b) Haber cooperado plena, continua y diligentemente a lo largo de todo el procedimiento de investigación.
- c) Haber facilitado información veraz y relevante, medios de prueba o datos significativos para la acreditación de los hechos investigados, sin que haya procedido a la destrucción de estos o a su ocultación, ni haya revelado a terceros, directa o indirectamente su contenido.
- d) Haber procedido a la reparación del daño causado que le sea imputable.

Si estos requisitos no se cumplen en su totalidad, incluida la reparación parcial del daño, quedará a criterio del Responsable del Sistema la posibilidad de atenuar la sanción que habría correspondido a la infracción cometida, siempre que el informante o autor de la revelación no haya sido sancionado anteriormente por hechos de la misma naturaleza que dieron origen al inicio del procedimiento.

La atenuación de la sanción podrá extenderse al resto de los participantes en la comisión de la infracción, en función del grado de colaboración activa en el esclarecimiento de los hechos, identificación de otros participantes y reparación o minoración del daño causado, apreciado por el órgano encargado de la resolución. En cualquier caso, la adopción de cualquiera de las anteriores decisiones deberá constar debidamente motivada por parte del Responsable del Sistema e incluida dentro del escrito de resolución.

10. TRATAMIENTO DE DATOS PERSONALES, CONSERVACIÓN, CUSTODIA Y ARCHIVO DE LA INFORMACIÓN

El acceso a los datos personales contenidos en el Sistema interno de información 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.
- b) Los encargados del tratamiento que eventualmente se designen.
- c) El delegado de protección de datos.

El Responsable del Sistema mantendrá actualizado el Libro-Registro de Comunicaciones con todas las informaciones recibidas, así como, en su caso, las investigaciones internas llevadas a cabo y las medidas adoptadas durante los plazos que, de acuerdo con la normativa aplicable, se encuentren legalmente permitidos en cada caso.

El citado registro, así como los tratamientos realizados por los intervinientes en la tramitación de las Comunicaciones recibidas a través del Sistema Interno de Información, cumplirá con las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad de los datos personales adecuado al riesgo y en su caso, aquellas previstas por la normativa sobre protección de datos que resulte de aplicación. Por lo que se refiere a la información comprendida bajo el registro, la misma se mantendrá actualizada en todo momento e incluirá, al menos, los siguientes datos:

- Fecha de recepción de la comunicación.
- Medio a través del cual se ha recibido la comunicación.
- Datos del denunciado y, si se conociesen, del Informador.
- Resumen de la naturaleza de la Comunicación y hechos sobre los que se aprecia el incumplimiento.
- Fechas de información a las partes implicadas.
- Documentación utilizada en la investigación.

Los datos personales relativos a las informaciones 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 cualquier caso, no se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar la información recibida, procediéndose a su eliminación sin dilación.

Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda

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 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.

Los datos personales relativos a Comunicaciones que no entren dentro del alcance del Sistema Interno de Información, no sean necesarios para el desarrollo de la investigación y/o no sean objeto de investigación, se suprimirán sin demora, con excepción de su puesta a disposición de las Administraciones Públicas u Órganos Jurisdiccionales, en caso de que pudieran ser necesarios para la atención de posibles responsabilidades durante los periodos de prescripción correspondientes. Tras ello, se procederá a la supresión física de los datos.

11. COMUNICACIÓN DEL PROTOCOLO

El presente Protocolo estará disponible en la web corporativa.

Puesto que el cumplimiento de las normas y estándares éticos compromete a toda la organización y constituye un objetivo estratégico para la misma, se espera que todo el personal conozca y respete el contenido de este Protocolo, para lo que se desarrollaran acciones de comunicación, formación y sensibilización para su oportuna y adecuada comprensión y puesta en práctica.

El SMAP reaccionará de forma inmediata ante eventuales incumplimientos de lo establecido en este Protocolo, conforme a lo previsto en su normativa interna y dentro de los parámetros establecidos en la legislación vigente.

12. APROBACIÓN, ACTUALIZACIÓN Y REVISIÓN

Este Protocolo ha sido aprobado por el Consejo de Administración del SMAP en la reunión de día 18.01.2024.

A partir de este momento se encuentra plenamente en vigor en todos sus términos, debiéndose mantener actualizado. Para ello será revisado de forma ordinaria con periodicidad anual y, de forma extraordinaria, cada vez que se produzcan variaciones en los objetivos estratégicos o legislación aplicable.

Corresponde a la Unitat de Seguiment de Riscos Penals valorar cualquier propuesta de modificación. Esta propuesta de modificación, siempre que suponga cambios sustanciales en el protocolo, deberá ser aprobada por el Comité de Compliance del SMAP.