



PROTOCOLO DE GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN

SIC24 SECURITY SYSTEMS, S.L.

Member of CISQ Federation



ÍNDICE

OBJETO DEL SISTEMA INTERNO DE INFORMACIÓN	4
ÁMBITO DE APLICACIÓN	5
FORMA DE PRESENTACIÓN DE DENUNCIAS	6
RECEPCIÓN DE LA DENUNCIA	7
▶ ACUSE DE RECIBO	7
▶ RECEPCIÓN Y REGISTRO	7
▶ ANÁLISIS PARA SU ADMISIÓN O INADMISIÓN	7
INVESTIGACIÓN	8
▶ MEDIOS DE INVESTIGACIÓN:	9
▶ EMISIÓN DE INFORME:	10
MEDIDAS	10
PROTECCIÓN AL DENUNCIANTE FRENTE A REPRESALIAS	11
CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL	11
VIGENCIA	12



OBJETO DEL SISTEMA INTERNO DE INFORMACIÓN

De conformidad con la legalidad vigente, y en aras de fomentar una cultura corporativa basada en el cumplimiento ético y normativo, así como para prevenir, descubrir y reaccionar frente a las infracciones de la ley, del Código Ético y del resto de normas internas, la Compañía habilita un protocolo de gestión del Sistema Interno de Información.

Su objetivo es establecer un procedimiento para la gestión del Sistema Interno de Información y todas las informaciones que se reciban por parte de empleados, administradores, socios, proveedores, así como otras personas interesadas sobre hechos contrarios a la legalidad, al Código Ético y/o a las normas internas. Para posibilitar esa labor de prevención, resulta de gran importancia la cooperación de todos en la detención de posibles conductas irregulares.

La existencia de dicho Sistema Interno no impide la presentación de denuncias por otros canales externos de ámbito europeo, estatal o autonómico existentes, como la Autoridad Independiente de Protección al Informante o ante las autoridades u órganos autonómicos correspondientes.

El presente protocolo ha sido elaborado con respeto a las directrices y principios fijados por la Directiva (UE) 1937/2019 de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre las infracciones del Derecho de la Unión ("Directiva Whistleblowing") y en la transposición de la misma, la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre las infracciones normativas y de lucha contra la corrupción ("Ley de protección del informante").

ÁMBITO DE APLICACIÓN

Todo aquel que tenga conocimiento de cualquier incumplimiento de la normativa legal vigente, que contravenga los compromisos recogidos en el Código Ético o que vulneren las políticas, normas o procedimientos de la sociedad, tiene el deber de denunciar tales conductas a través del Sistema Interno de Información de manera diligente.

A tenor de lo anterior, la Compañía canalizará y facilitará la **formulación segura** de cualquier comunicación sobre:

- Cualesquiera acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea, siempre y cuando:
- Entren dentro del ámbito de aplicación de los actos de la Unión Europea enumerados en el anexo de la Directiva (UE) 2019/1937 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.
- Afecten a los intereses financieros de la Unión Europea tal y como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE);
- Incidan en el mercado interior, como se contempla en el artículo 26.2 del TFUE.
- Todas las acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave o cualquier vulneración del resto del ordenamiento jurídico.
- Cualquier acción contraria a las políticas, protocolos, procedimientos y códigos internos que la Compañía tenga instaurados en materia de Compliance.
- Cualquier indicio, sospecha o evidencia de comportamiento no ético, discriminatorio, contrario a la igualdad de las personas y posible acoso laboral y/o sexual.
- Cualquier operación sospechosa, incidencia o riesgo en materia de “Prevención del Blanqueo de Capitales y financiación del terrorismo”, fraude, corrupción o existencia de conflictos de interés.

El Sistema Interno de Información debe entenderse como un instrumento que permita la comunicación de irregularidades o incumplimientos. Por ello, no debe emplearse de manera indiscriminada, sino para los fines que ha sido concebido.

El Sistema se articula como una herramienta confidencial (vid. Punto 7) y cuya utilización no conllevará represalias (vid. Punto 8).

FORMA DE PRESENTACIÓN DE DENUNCIAS

De conformidad con lo establecido en el artículo 8 de la Ley 2/2023, de 20 de febrero, se ha nombrado al responsable de Recursos Humanos como Responsable del Sistema Interno de Información.

La gestión del sistema se llevará de manera conjunta con el equipo externo del Departamento de Compliance del despacho Rebés-Ferrer.

En adelante, dentro de este protocolo se hará mención a las tareas que el Responsable del Sistema llevará a cabo en el contexto de una investigación interna. No obstante, cabe destacar que estas funciones podrán ser llevadas a cabo por el despacho externo.

Las denuncias pueden llevarse a cabo de forma anónima, y de no ser así, se reservará la identidad del informante. Se podrán interponer de manera escrita y/o de manera verbal por las siguientes vías:

- El canal denuncias: canalcomunicacion@sic24.com
- Mediante correo postal:
 - Departamento de Compliance, Rebés-Ferrer Travessera de Gràcia, 18, 4ª 08021
- Llamada telefónica:
 - Responsable del sistema interno de información: [648 688 552](tel:648688552)
 - Departamento de Compliance, Rebés-Ferrer: [933 68 27 38](tel:933682738)
- Reunión presencial con el Responsable del Sistema, a solicitud del informante en un plazo máximo de 7 días.

Cuando se traten de denuncias verbales, previo consentimiento del informante, se documentarán diligentemente mediante una grabación de la conversación en un formato duradero, seguro y accesible o bien, a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla, pudiendo el informante comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

Las denuncias que se realicen a través de estas vías, es recomendable que contengan, como mínimo, los siguientes elementos:

- Identidad del denunciado/a: nombre y apellidos, así como aquellos otros datos que se conozcan y se consideren relevantes para la identificación del/de la presunto/a infractor/a.
- Motivo de la denuncia: descripción de los hechos o circunstancias que a criterio del/de la denunciante constituyen un incumplimiento o irregularidad.
- Evidencias concretas que den soporte a la denuncia: todos aquellos documentos de los que se disponga que soporten la creencia de la comisión de la irregularidad descrita en el motivo de la denuncia.
- En su caso, el denunciante podrá indicar un domicilio, correo electrónico o lugar seguro a los efectos de recibir notificaciones. Asimismo, en cualquier momento podrá el denunciante renunciar expresamente a la recepción de cualquier comunicación respecto de las actuaciones realizadas a consecuencia de la denuncia.

RECEPCIÓN DE LA DENUNCIA

► ACUSE DE RECIBO

Tras la recepción de una denuncia, se deberá acusar recibo a la persona denunciante de su correcta recepción, por la misma vía por la que fue interpuesta, en un plazo no superior a 7 días hábiles a contar desde el día siguiente a su recepción, salvo que lo anterior no resulte posible por ser la denuncia anónima, la persona haya renunciado a recibir comunicaciones o que ello pueda poner en peligro la confidencialidad de la comunicación.

En el caso de que se trate de una denuncia por una conducta de las previstas en el Protocolo para la prevención y abordaje del acoso y violencia en el trabajo se activará el mismo siguiendo el procedimiento que en él se detalla.

► RECEPCIÓN Y REGISTRO

La Empresa contará con un libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad previstos en la Ley.

Siguiendo con lo anterior, de cada denuncia recibida se abrirá un expediente que se tendrá que registrar en el Sistema de Gestión de Denuncias, siéndole asignado un código de identificación. Este Sistema estará en una base de datos segura y de acceso restringido.

Se tendrá que registrar a lo largo del proceso:

- Fecha y forma de recepción de la denuncia
- Código de identificación
- Personas que de una forma u otra figuren en la misma.
- Breve resumen de los hechos
- Admisión o inadmisión de la denuncia
- Todas las actuaciones desarrolladas
- Pruebas practicadas
- Medidas adoptadas
- Fecha de cierre

► ANÁLISIS PARA SU ADMISIÓN O INADMISIÓN

Una vez registrada la denuncia, el Responsable del Sistema debe realizar un primer juicio de idoneidad a los efectos de determinar si la denuncia expone de manera clara y evidente hechos constitutivos o no de infracción, irregularidad o incumplimiento de la normativa legal vigente, los compromisos recogidos en el Código Ético o las políticas, normas o procedimientos de la sociedad. En función del resultado deberá decidir si:

- **Inadmitir la denuncia**, por medio de resolución motivada, cuando los hechos descritos sean de naturaleza distinta a los recogidos para la admisión de la denuncia.
- **Admitir a trámite la denuncia**. Se propondrá cuando de los hechos denunciados, se desprendan sospechas de suponer un acto ilícito o contrario a los principios y valores de la Empresa. La

admisión de la denuncia será notificada al denunciante salvo que la denuncia fuera anónima, la persona hubiera renunciado a recibir comunicaciones o se pudiera poner en peligro la confidencialidad de la comunicación.

Tras la admisión de la denuncia, el Responsable del Sistema podrá optar entre llevar la investigación o designar un instructor en el que delegar la fase de investigación. En todo caso, será responsabilidad del Responsable del Sistema informar a Gerencia.

En caso de que la denuncia se dirija contra el Responsable del Sistema persona física, o en caso de concurrir cualquier circunstancia que genere un conflicto de interés, se abstendrá de intervenir en la decisión de admisión o inadmisión de la denuncia, así como de todo lo concerniente al proceso de investigación, evaluación y decisión sobre la misma y su gestión será ejercida en exclusiva por el asesor externo del departamento de Compliance del despacho Rebés-Ferrer.

Por último, el Responsable del Sistema o el instructor que se designe tiene el deber de guardar la más absoluta confidencialidad en relación con cualquier denuncia que, recibida, sea o no desestimada, en lo referente al/a la denunciante y al/a la denunciado/a, absteniéndose de promover cualquier tipo de represalias al/a la denunciante.

INVESTIGACIÓN

Tras la recepción de la denuncia y la admisión de la misma, el Responsable del Sistema o el instructor que se designe ordenará la apertura de la correspondiente investigación interna, con el fin de:

- a) Esclarecer los hechos denunciados
- b) Identificar a los responsables de las conductas denunciadas
- c) Recopilar las pruebas pertinentes para su descubrimiento

El plazo máximo en el que se deberá desarrollar la investigación **no podrá superar los 3 meses** desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante, 3 meses a partir del vencimiento del plazo de 7 días después de efectuarse la comunicación. Se podrá autorizar la prórroga extraordinaria hasta 3 meses más, cuando resulte proporcional a la naturaleza y dificultad de los hechos objeto de la investigación dictando una resolución motivada a tales efectos.

En el proceso de investigación, el Responsable del Sistema o el instructor que se designe realizará todas aquellas acciones y consultas que considere necesarias encaminadas a la averiguación de la exactitud y veracidad de la información recibida, así como encaminadas al esclarecimiento de los hechos.

Acordada la apertura del expediente, el Responsable del Sistema o el instructor que se designe se pondrá en contacto con el denunciado, identificándose ante este como el encargado de la investigación de la denuncia e informándole sucintamente acerca de los hechos que se le atribuyen y de los principales hitos que se pueden producir durante la investigación. Asimismo, en dicha comunicación, se le informará de su posibilidad de presentar alegaciones por escrito y se le informará del tratamiento de sus datos personales.

En ningún caso se notificará a los sujetos investigados la identidad del denunciante ni se hará entrega de la denuncia, todo ello en aras de la protección del denunciante.

► MEDIOS DE INVESTIGACIÓN:

En la fase de instrucción, se podrán realizar todas las actuaciones jurídicamente lícitas y válidas para la averiguación de los hechos objeto de denuncia, respetando siempre el principio de proporcionalidad, debiendo respetarse siendo que la medida sea excepcional (no existan otras actuaciones investigadoras menos gravosas para alcanzar el objetivo perseguido), necesaria (sin su práctica se podrá comprometer la investigación) e idónea (deberá servir a los fines de la investigación).

Todos los empleados/as y miembros de los órganos directivos de la Empresa están obligados a prestar la colaboración requerida por el órgano de instrucción para, en su caso, colaborar en la investigación y su intervención tendrá carácter estrictamente confidencial.

Serán medios lícitos de investigación los siguientes:

1. **Entrevista a la persona o personas investigadas.** precedida de lectura de derechos y garantías que le asisten:
 - o Derecho a ser informado de los hechos objeto de investigación y ser oída en cualquier momento.
 - o Derecho a cotejar el expediente de investigación, sin revelar información que pudiera identificar a la persona informante.
 - o Derecho a ser informado de si se procederá a la grabación y registro de la entrevista.
 - o Derecho a formular alegaciones por escrito y a proponer diligencias de investigación.
 - o Derecho a la presunción de inocencia y al honor
2. **Entrevista con el denunciante** si resulta posible, deberá ir precedida del correspondiente aviso de la prohibición de recibir cualquier tipo de represalia o tentativa de represalia a consecuencia de la denuncia interpuesta. Indicando la posibilidad de mantener la comunicación durante toda la investigación y solicitar a la persona información adicional.
3. **Entrevista a testigos** que pudieran tener conocimiento o fueran testigo de los hechos denunciados.
4. **Examen de cualquier tipo de documentación y requerimiento de la misma a las personas físicas o jurídicas correspondientes.**
5. **Recuperación y análisis de la información contenida en dispositivos electrónicos, mediante el uso de herramientas de software y hardware que preserven la integridad de las pruebas, con respeto absoluto a la legalidad vigente y a lo dispuesto en el Código Ético.**
6. **Si fuera indispensable para el esclarecimiento de los hechos, adoptar medidas de vigilancia a través de detectives o medios informáticos, telemáticos o audiovisuales, siempre que los mismos atiendan a criterios de razonabilidad, idoneidad y proporcionalidad, velando en todo momento por el derecho a la intimidad del trabajador y por el derecho al secreto de las comunicaciones.**
7. **Solicitar ayuda externa de otros profesionales.**
8. **Cualesquiera otras diligencias que el investigador estime necesarias para el esclarecimiento de los hechos.**

Al finalizar todas aquellas entrevistas que se lleven a cabo, se levantará acta sucinta de la reunión y se firmará por el entrevistado en prueba de su conformidad. También se recogerán evidencias de todas las actuaciones que se realicen.

► EMISIÓN DE INFORME:

Una vez concluidas todas las actuaciones, el Responsable del Sistema o el instructor que se designe procederá a la emisión de un informe de los procedimientos realizados. Si la investigación la ha realizado el instructor y, por tanto, es la persona que emite el informe, deberá elevarlo al Responsable del Sistema.

Este informe contendrá al menos:

- Una exposición de los hechos denunciados junto con el código de identificación de la denuncia y la fecha de su recepción.
- Las actuaciones realizadas con el fin de esclarecer los hechos, la valoración de las pruebas practicadas y de los indicios obtenidos.
- Las conclusiones de las instrucciones, con la identificación de la debilidad que, en su caso, haya provocado la situación y propuesta de plan de acción frente a la debilidad identificada.

MEDIDAS

Una vez emitido el informe, el Responsable del Sistema será el responsable de tomar las medidas internas oportunas, sin perjuicio de las responsabilidades administrativas y de otra índole que le puedan corresponder a los Juzgados y Tribunales.

Adoptará, a la mayor brevedad posible, alguna o algunas de las siguientes decisiones:

- **Archivo del expediente:** valorar si de la investigación no se derivan datos que exijan más actuaciones al no existir indicios suficientes de la presunta comisión de hecho delictivo, o en todo caso, por resultar hechos que por su escasa relevancia no deban motivar ulteriores actuaciones. En ese caso, se acordará el archivo del expediente acompañado de una exposición razonada y detallada, notificando dicha decisión al denunciante y, en su caso, al denunciado.
- **Traslado a la autoridad administrativa correspondiente.** Si los hechos objeto de denuncia pudiesen ser objeto de una infracción administrativa, se pondrá en conocimiento del organismo correspondiente para incoación del oportuno procedimiento sancionador.
- En caso de que los hechos puedan dar lugar a una responsabilidad disciplinaria de algún empleado de la Empresa, se dará **traslado del informe a la Dirección del departamento de Recursos Humanos** a los efectos de que este adopte, en su caso, las medidas que resulten de aplicación de acuerdo con la normativa laboral vigente en cada momento.
- **Traslado al Ministerio Fiscal:** Si los hechos objeto de la denuncia pudiesen ser constitutivos de delito, los pondrá en conocimiento de la Fiscalía. Si el delito afectase a los intereses financieros de la Unión, lo remitirá a la Fiscalía Europea.

PROTECCIÓN AL DENUNCIANTE FRENTE A REPRESALIAS

Las personas que formulen cualquier clase de comunicación de incumplimiento, según lo aquí previsto y de buena fe, quedan protegidas frente a cualquier tipo de represalia, discriminación y penalización por motivo de las comunicaciones realizadas. Así las cosas, se prohíben expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia

En sentido explicativo, se entiende como 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.

CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Esta Empresa documentará por escrito todas las actuaciones llevadas a cabo en el marco de las comunicaciones de incumplimientos y la tramitación del expediente correspondiente y lo conservará cumpliendo con los requisitos de confidencialidad y con los plazos de conservación establecidos por otras normativas de obligado cumplimiento.

El tratamiento de los datos personales realizado en virtud de las actuaciones llevadas a cabo en el marco del presente Protocolo se regirán por lo dispuesto en el RGPD, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los derechos digitales, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, y en la normativa aplicable. En este sentido, no se recopilarán datos personales cuya pertinencia no resulte manifiesta y necesaria para la averiguación y descubrimiento de los hechos objeto de denuncia.

Con el objeto de conseguir un máximo nivel de implicación y seguridad para con la persona que desee poner en conocimiento una infracción o conducta irregular a través del Sistema Interno de Información, así como para con la persona afectada, la Empresa pondrá los medios necesarios para que dichas comunicaciones vertidas al Sistema Interno de Información sean tratadas con la mayor confidencialidad por parte de todos los implicados en la investigación y resolución de la misma.

Las personas que efectúen una comunicación a través del canal ético manifiestan y garantizan que los datos personales proporcionados son verdaderos, exactos, completos y actualizados, y mantendrán indemne a la Empresa de cualesquiera responsabilidades se puedan derivar por el incumplimiento de dichas manifestaciones y garantías.

En todo caso, los datos que sean objeto de tratamiento podrán conservarse 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 acreditara que la información facilitada o parte de ella no es veraz, se procederá 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.

- No obstante lo anterior, el responsable del sistema será el encargado de archivar y custodiar toda la documentación resultante, en el libro-registro, durante diez años desde la recepción de la comunicación o denuncia.

- En cualquier caso, los datos se conservarán de forma bloqueada, es decir, se identificarán y reservarán con el fin de impedir su tratamiento excepto para su puesto a disposición de las Administraciones Públicas, Jueces y Tribunales. 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 prevista en el artículo 31 de la Ley Orgánica 3/2018, de 5 de diciembre.

El denunciante podrá ejercitar los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento, en los supuestos legalmente permitidos, así como el derecho a la portabilidad de los datos, podrán ejercerse, en los términos especificados por la normativa vigente, ante la Empresa, mediante comunicación escrita dirigida al correo electrónico canalcomunicacion@sic24.com

En cuanto a la gestión y archivo tanto de los datos personales como de toda la información facilitada por el denunciante, serán incluidos en un fichero automatizado de datos titularidad de la Empresa, mantenido bajo la responsabilidad del Responsable de Protección de Datos de la Empresa y protegido por las medidas de seguridad adecuadas de acuerdo con la legislación vigente.

VIGENCIA

El presente Protocolo tendrá una vigencia indefinida, todo ello sin perjuicio de las posibles modificaciones y mejoras que en el mismo puedan introducirse.