PROCEDIMIENTO DE GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN

CEPYME

CONFEDERACIÓN ESPAÑOLA DE LA PEQUEÑA Y MEDIANA EMPRESA

ÍNDICE

I. INTRODUCCIÓN

El art.31 Bis Punto 5, apartado 4.º del Código Penal, entre otros requisitos de un Modelo de Organización y Gestión para la Prevención de Delitos, establece que las personas jurídicas habrán de imponer "*la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención*".

Por otra parte, 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 establece la obligación de constituir un Canal interno de comunicaciones con el objetivo de facilitar un medio a través del cual realizar la comunicación de conductas irregulares o sospechosas.

Aquellas personas que informen de posibles incumplimientos quedarán protegidas por las salvaguardas contempladas en la Ley 2/2023 siempre y cuando se cumplan los requisitos establecidos en cuanto ámbito material y personal.

Bajo estas premisas, **CONFEDERACIÓN ESPAÑOLA DE LA PEQUEÑA Y MEDIANA EMPRESA (CEPYME),** en el marco de su Modelo de Organización y Gestión para la Prevención de Delitos (en adelante, Modelo), basado en la UNE 19.601, dispone un Sistema Interno de Información que incluye un Canal de comunicaciones (en adelante, "el Canal"), con el objetivo de facilitar un medio a través del cual realizar la comunicación de conductas irregulares o sospechosas o realizar consultas en relación con el funcionamiento del Modelo.

El Sistema Interno en general y el Canal en particular se configuran como parte indispensable de la cultura de cumplimiento y de la información y de las infraestructuras de integridad de la Organización, con la vocación de prevenir o detectar amenazas al interés público.

Se incentivará el uso del canal de comunicación garantizando a los interesados que la información que aporten será tratada de manera confidencial dentro de la propia empresa y sin riesgo de represalias.

El Sistema interno de información será el cauce preferente para informar sobre acciones u omisiones que queden dentro de su alcance, siempre que se pueda tratar de manera efectiva la infracción y si el informante considera que no hay riesgo de represalia.

El sistema ha de promover asimismo unos resultados idóneos para la correcta implementación del Modelo en la organización, buscando:

a) alentar y facilitar la comunicación de irregularidades;
b) apoyar y proteger a los informantes y otras personas involucradas;
c) garantizar que las comunicaciones de irregularidades se tramiten de manera adecuada y oportuna;
d) mejorar la cultura organizacional, la gobernanza y la prevención de las irregularidades.

Los beneficios potenciales para la organización incluyen:

a) permitir que la organización identifique y aborde las irregularidades lo antes posible;
b) ayudar a prevenir o reducir al mínimo la pérdida de activos y ayudar a la recuperación de activos perdidos;
c) garantizar el cumplimiento de las políticas, los procedimientos y las obligaciones jurídicas y sociales de la organización;
d) atraer y retener a personal comprometido con los valores y la cultura de la organización; y
e) demostrar a la sociedad, a los mercados, a los reguladores, a los propietarios y a otras partes interesadas prácticas de gobernanza sólidas y éticas.

Un sistema interno de información eficaz fomentará la confianza de la organización, mediante:

a) demostrar el compromiso del liderazgo para prevenir y abordar las irregularidades;
b) alentar a las personas a que presenten pronto informes de irregularidades;
c) reducir y prevenir el tratamiento perjudicial de los informantes y otras personas implicadas; y
d) fomentar una cultura de apertura, transparencia y responsabilidad.

II. OBJETIVO DEL PROCEDIMIENTO

El presente Procedimiento pretende constituir la guía de actuación ante una comunicación que entre a través de los canales habilitados y su posterior gestión.

De esta manera, queda establecido cómo gestionar la información recibida, qué decisiones adoptar y qué proceso de investigación seguir, tanto en fase previa de evaluación de la información recibida, en la actuación pre-procesal en caso de apertura de expediente de investigación y también, teniendo en cuenta la eventual posibilidad de un procedimiento penal.

La regulación de la reacción ante la comunicación de posibles incumplimientos o irregularidades constituye una parte importante de las políticas de cumplimiento normativo, en una organización que se ha autoimpuesto altos estándares éticos y una clara vocación de crear una "Cultura de Cumplimiento" en su seno.

Todos los miembros de la Organización tienen el deber de colaborar en los procesos de investigación que se abran.

La Política del Sistema Interno de Información está a disposición en: https://cepyme.canalhelas.com/home.

III. CANAL INTERNO DE INFORMACIÓN.

El Sistema Interno de Información incluye un Canal interno para posibilitar la presentación de información respecto de las infracciones previstas en el alcance definido y deberá permitir realizar comunicaciones por escrito o verbalmente, o de las dos formas.

En ese sentido, el medio determinado por la Organización para recibir y gestionar comunicaciones es/son el/los siguiente/s:

a) Por escrito a través de:

- Correo electrónico a: canaldecomunicaciones@cepyme.es
- A través de la página web https://cepyme.canalhelas.com/home.
- Correo postal a la dirección C/Diego de León, 50 - 28006 MADRID

b) Verbalmente a través de:

- Reunión presencial con el Responsable del Sistema Interno.

Las comunicaciones verbales deberán documentarse de alguna de las maneras siguientes, previo consentimiento del informante:

- mediante una grabación de la conversación en un formato seguro, duradero y accesible
- a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.

Se informará al interesado acerca del tratamiento de sus datos conforme a la normativa de protección de datos y se le ofrecerá la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

Se admitirá la presentación y posterior tramitación de **comunicaciones anónimas.**

Por último, a quienes realicen la comunicación a través de este medio se les informará, de forma clara y accesible, sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

IV. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN.

El órgano de administración u órgano de gobierno de la Organización es el competente para la designación de una persona física responsable de la gestión de dicho sistema o «Responsable del Sistema», y de su destitución o cese, pudiendo optarse porque el Responsable del Sistema sea un órgano colegiado, debiendo entonces éste delegar en uno de sus miembros las facultades de gestión del Sistema interno de información y de tramitación de expedientes de investigación.

Tanto el nombramiento como el cese del Responsable deberán ser notificados a la Autoridad Independiente de Protección del Informante, A.I.P.I., o, en su caso, a las autoridades u órganos competentes de las comunidades autónomas, en el ámbito de sus respectivas competencias, en el plazo de los

diez días hábiles siguientes, especificando, en el caso de su cese, las razones que han justificado el mismo.

El Responsable deberá desarrollar sus funciones de forma independiente y autónoma respecto del resto de los órganos de la organización, 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.

Al pertenecer la Organización al sector privado, el Responsable del Sistema podrá ser un directivo de la entidad, que ejercerá su cargo con independencia del órgano de administración o de gobierno de esta.

Cuando la naturaleza o la dimensión de las actividades de la entidad no justifiquen o permitan la existencia de un directivo Responsable del Sistema, será posible el desempeño ordinario de las funciones del puesto o cargo con las de Responsable del Sistema, tratando en todo caso de evitar posibles situaciones de conflicto de interés.

Bajo estas premisas, la Organización ha determinado que la función de Responsable del Sistema Interno de Información sea asumida por el la Dirección de Recursos Humanos, lo cual queda debidamente documentado en el correspondiente documento de nombramiento.

V. ÁMBITO MATERIAL DEL SISTEMA INTERNO DE INFORMACIÓN.

Podrán trasladarse a través del canal, y ser gestionadas conforme al Sistema Interno de Información, comunicaciones relativas a:

a) Acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea siempre que:
    1. Entren dentro del ámbito de aplicación de los actos de la Unión Europea enumerados en el anexo de la Directiva (UE) 2019/1937[1];
    2. Afecten a los intereses financieros de la UE tal y como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE);
    3. Incidan en el mercado interior, tal y como se contempla en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión Europea en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades o con prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades.
b) Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave. En todo caso, se entenderán comprendidas todas aquellas infracciones penales o administrativas graves o muy graves que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.

[1] **https://www.boe.es/doue/2019/305/L00017-00056.pdf**

c) Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa menos grave o leve.
d) Acciones u omisiones de normas, políticas o procedimientos internos de obligado cumplimiento para los integrantes de la Organización y cuya inobservancia pueda suponer un grave daño para la entidad y pueda derivar en sanciones disciplinarias en el ámbito laboral.

Las personas que informen de conductas relativas a este último extremo o que no sean constitutivas de infracciones graves o muy graves no gozarán legalmente de la protección que otorga a los informantes la Ley 2/2023 reguladora de protección de las personas que informen sobre infracciones normativas y de la lucha contra la corrupción.

No obstante, la Organización, como muestra de su compromiso y de forma proactiva, reconocerá el derecho a la protección a los informantes de Acciones u omisiones de normas, políticas o procedimientos internos de obligado cumplimiento comprometiéndose igualmente a no aplicar represalias sobre dichas personas.

De forma orientativa, se podrán comunicar irregularidades o incumplimientos relativos a los siguientes ámbitos:

- Contratación pública.
- Servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo.
- Seguridad de los productos y conformidad.
- Seguridad del transporte.
- Protección del medio ambiente.
- Protección frente a las radiaciones y seguridad nuclear.
- Seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales.
- Salud pública.
- Protección de los consumidores.
- Protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información.
- Infracciones que afecten a los intereses financieros de la Unión Europea.
- Infracciones relativas al mercado interior en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades.

VI. ÁMBITO PERSONAL.

Las personas que podrán hacer uso del canal son aquellas que hayan obtenido información sobre infracciones en un contexto laboral o profesional, comprendiendo en todo caso:

a) Las personas que tengan la condición de empleados;

b) Los autónomos;

c) Los accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión, incluidos los miembros no ejecutivos;

d) Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

Dado que la organización ha implantado el Modelo cumpliendo los requisitos de la Certificación UNE 19601 de Sistemas de Gestión de Compliance, el canal queda abierto igualmente a terceras partes o socios de negocios tales como Clientes, Proveedores, Colaboradores y cualquier tercero relacionado.

VII. CONTENIDO MÍNIMO DE LAS COMUNICACIONES

La comunicación deberá contener, en la medida de lo posible, los siguientes extremos:

- Descripción de las conductas supuestamente irregulares, contrarias a la legalidad o a lo establecido en el Código u otras normas internas.
- Posibles personas implicadas.
- Fechas aproximadas de comisión de los hechos.
- Medios a través de los cuales se han realizado las conductas.
- Áreas de negocio afectadas.
- Procesos relevantes afectados (p.ej. contratación, contabilidad, tesorería…).
- Documentos o evidencias de los hechos.

En cualquier caso, se recomienda que la comunicación sea lo más descriptiva y detallada posible, facilitando de esta forma al receptor la identificación de la/s persona/s o departamento/s implicado/s.

Con el fin de decidir sobre su admisión a trámite, se podrá solicitar al informante la aclaración o complemento de los hechos, aportando aquella documentación o datos que pudieran ser necesarios para acreditar la existencia de la conducta irregular.

VIII. CONDICIONES DE PROTECCIÓN.

Se garantiza la protección de aquellas personas que realicen una comunicación de buena fe y de forma honesta y transmitan al Sistema Interno de Información las conductas que estimen irregulares o ilícitas.

Así, quedarán protegidas aquellas personas que, teniendo motivos razonables para creer, a la luz de las circunstancias y de la información de que dispongan en el momento de la comunicación, que los hechos que comunican o denuncian son ciertos.

Esta protección no se perderá, aunque el informante comunique información inexacta por un error cometido de buena fe.

La motivación personal que pudiera tener el informante al realizar la comunicación no se tendrá en cuenta para otorgar esta protección.

Especialmente quedan protegidas aquellas personas que reporten a través de este canal con motivo de sus actividades laborales relacionadas con la Organización quedando protegidas frente al riesgo de represalias laborales, por ejemplo, por incumplir la obligación de confidencialidad o de lealtad.

Esta protección se aplicará no solamente a la persona que tenga la condición de «trabajador» a tiempo completo, sino que quedan incluidos los trabajadores a tiempo parcial y los trabajadores con contratos de duración determinada o con un contrato de trabajo o una relación laboral con una empresa de trabajo temporal.

Igualmente, esta protección se aplicará en los siguientes casos:

a) Personas que aun no habiendo sido todavía contratadas participan en procesos de selección, personas que hayan finalizado una relación laboral, o personal como becarios, voluntarios trabajadores en periodos de formación, es decir, personas que puedan sufrir represalias, por ejemplo, en forma de referencias de trabajo negativas, inclusión en listas negras o boicot a su actividad empresarial.

b) Representantes legales de las personas trabajadoras en su labor de asesoramiento del informante.

c) Personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso.

d) Personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante.

e) Personas jurídicas, para las que trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa el informante.

IX. MEDIDAS DE APOYO.

La Ley 2/2023 reconoce que las personas que comuniquen o revelen infracciones podrán acceder a las medidas de apoyo siguientes y que habrán de ser prestadas por las Autoridades competentes:

a) Información y asesoramiento completos e independientes, fácilmente accesibles y gratuitos, sobre los procedimientos y recursos disponibles, protección frente a represalias y derechos de la persona afectada.

b) Asistencia efectiva por parte de las autoridades competentes ante cualquier autoridad pertinente implicada en su protección frente a represalias, incluida la certificación de que pueden acogerse a protección al amparo de la presente ley.

c) Asistencia jurídica en los procesos penales y en los procesos civiles transfronterizos de conformidad con la normativa comunitaria.

d) Apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la Autoridad Independiente de Protección del Informante, A.A.I. tras la valoración de las circunstancias derivadas de la presentación de la comunicación.

Todo ello, con independencia de la asistencia que pudiera corresponder al amparo de la Ley 1/1996, de 10 de enero, de asistencia jurídica gratuita, para la representación y defensa en procedimientos judiciales derivados de la presentación de la comunicación o revelación pública.

Estas medidas de apoyo han de ser prestadas por las Autoridades competentes y así se informará a los interesados.

X. MEDIDAS DE PROTECCION FRENTE A REPRESALIAS

La protección reconocida en la Ley 2/2023 incluye:

a) No considerar que el informante infringe restricciones sobre la revelación que realice ni considerar que incurre en responsabilidad siempre que tuviera motivos razonables para pensar que es necesaria para poner en conocimiento de la organización una acción u omisión de la normativa.
b) No incurrir 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.

Quedarán excluidas de toda protección aquellas personas que informen de forma malintencionada, frívola o abusiva, o comuniquen deliberada y conscientemente información incorrecta o engañosa, así como aquellas personas que comuniquen información que sea de dominio público, o rumores y habladurías no confirmados.

Esta medida no afectará a las responsabilidades de carácter penal.

Esta protección se extiende a la comunicación de informaciones realizadas por los representantes de las personas trabajadoras, aunque se encuentren sometidas a obligaciones legales de sigilo o de no revelar información reservada.

Todo ello sin perjuicio de las normas específicas de protección aplicables conforme a la normativa laboral.

Situaciones especiales:

- En los procedimientos ante un órgano jurisdiccional u otra autoridad relativos a los perjuicios sufridos por los informantes, una vez que el informante haya demostrado razonablemente que ha comunicado o ha hecho una revelación pública de conformidad con la ley y que ha sufrido un perjuicio, se presumirá que el perjuicio se produjo como represalia por informar o por hacer una revelación pública.
- En tales casos, corresponderá a la persona que haya tomado la medida perjudicial probar que esa medida se basó en motivos debidamente justificados no vinculados a la comunicación o revelación pública.
- En los procesos judiciales, incluidos los relativos a difamación, violación de derechos de autor, vulneración de secreto, infracción de las normas de protección de datos, revelación de secretos empresariales, o a solicitudes de indemnización basadas en el derecho laboral o estatutario, los informantes no incurrirán en responsabilidad de ningún tipo como consecuencia de comunicaciones o de revelaciones públicas protegidas por la misma.
- Dichas personas tendrán derecho a alegar en su descargo y en el marco de los referidos procesos judiciales, el haber comunicado o haber hecho una revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública era necesaria para poner de manifiesto una infracción.

XI. PROHIBICIÓN DE REPRESALÍAS.

Los informantes quedan protegidos contra toda forma represalia, incluida la tentativa o cualquier forma de amenaza, ya sea directa o indirecta, que se tome, se aliente o se tolere por parte de los propios compañeros de trabajo o directivos.

Aquellas personas que tomen alienten o toleren represalias contra un informante podrán ser sancionados disciplinariamente en aplicación de las disposiciones sancionadoras establecidas en el CÓDIGO ÉTICO Y DE BUEN GOBIERNO u otra normativa de aplicación como el Convenio Colectivo de aplicación o el Estatuto de los Trabajadores.

Se entiende como represalias, ya sean consumadas o en grado de tentativa o amenaza, las siguientes acciones:

a) suspensión, despido, destitución, extinción, o medidas equivalentes de la relación laboral y/o estatutaria,
b) degradación o denegación de ascensos,
c) modificación de las condiciones de trabajo: cambio de puesto, ubicación del lugar de trabajo, reducción salarial o cambio del horario de trabajo,
d) denegación de formación.
e) evaluación o referencias negativas con respecto a sus resultados laborales y profesionales,
f) imposición de cualquier medida disciplinaria, amonestación u otra sanción, incluidas las sanciones pecuniarias,
g) coacciones, intimidaciones, acoso u ostracismo,
h) discriminación, o trato desfavorable o injusto,
i) no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido,
j) no renovación o terminación anticipada de un contrato de trabajo temporal,
k) daños, incluidos a su reputación, en especial en los medios sociales, o pérdidas económicas, incluidas la pérdida de negocio y de ingresos,
l) inclusión en listas negras sobre la base de un acuerdo sectorial, informal o formal, que pueda implicar que en el futuro la persona no vaya a encontrar empleo en dicho sector,
m) terminación anticipada o anulación de contratos de bienes o servicios,
n) anulación de una licencia o permiso.

XII. MEDIDAS PARA LA PROTECCIÓN DE LAS PERSONAS AFECTADAS.

Las personas afectadas por la comunicación efectuada han de tener igualmente garantizados ciertos derechos durante todo el proceso, en concreto:

a) El derecho a la presunción de inocencia y al honor.
b) El derecho a ser oído, o de las acciones u omisiones que se le atribuyen, dentro de un plazo adecuado que permita no perjudicar la investigación.
c) El derecho a su propia y legítima defensa.
d) El acceso al expediente con las limitaciones establecidas normativamente.
e) La confidencialidad de sus datos personales y preservación de su identidad.
f) La confidencialidad de los hechos y del procedimiento.
g) Se reconocen determinados supuestos de exención y atenuación de la sanción que en su caso pudiese corresponder aplicar a las personas afectadas de demostrarse como ciertas las informaciones.

Supuestos de exención.

Cuando una persona que hubiera participado en la comisión de la infracción objeto de la información sea la que informe de su existencia con anterioridad a que hubiera sido notificada la incoación del procedimiento de investigación o sancionador, podrá quedar eximida de sanción administrativa que le corresponda siempre que cumpla 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

Supuestos de atenuación.

Cuando estos requisitos no se cumplan en su totalidad, incluida la reparación parcial del daño, quedará a criterio de la autoridad competente, previa valoración del grado de contribución a la resolución del expediente, 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.

Esto no se aplicará a las infracciones establecidas en la Ley 15/2007, de 3 de julio, de Defensa de la Competencia

XIII. PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES.

El órgano de administración u órgano de gobierno de la Organización es responsable de aprobar el presente procedimiento de gestión de informaciones. Por su parte, el Responsable del Sistema designado responderá de su tramitación diligente.

El ciclo de vida de cada comunicación ha de quedar regulado y documentado, desde su comunicación inicial hasta su resolución o archivo.

A. Fase previa y principios rectores.

1. Identificación de canales internos de información a los que se asocia.

El presente procedimiento de gestión se aplica a las informaciones que se comuniquen en el marco del Canal interno accesible a través de https://cepyme.canalhelas.com/home.

2. Información sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

- ✓ Autoridad Independiente de Protección del Informante (AIPI);
- ✓ Canal de información sobre fraudes o irregularidades que afecten a fondos europeos del Servicio Nacional de Coordinación Antifraude (SNCA). Ministerio de Hacienda y Función Pública del Gobierno de España.
- ✓ Oficina Europea de Lucha contra el fraude (OLAF)

3. Principios rectores del procedimiento

Teniendo en cuenta las posibles consecuencias penales de los hechos que pueden ser comunicados a través del canal, su gestión estará alineada con los principios rectores de los procedimientos judiciales:

- Documentación: sea cual sea la vía de entrada, el procedimiento de investigación habrá de quedar debidamente documentado por escrito, sin perjuicio de ciertas acciones que puedan ser verbales (por ej., entrevistas con testigos o el propio denunciante).
- Impulso de la investigación: una vez que se recibe una comunicación de hechos susceptibles de incumplimiento o infracción, la investigación dependerá ya de la voluntad de la organización, evitando así que el denunciante haga un mal uso del canal.
- Contradicción: durante la investigación se habrá de permitir en todo momento al denunciado que pueda ejercer su derecho de defensa.

4. Envío de acuse de recibo de la comunicación al informante

En el plazo de siete días naturales siguientes a la recepción de la comunicación, salvo que ello pueda poner en peligro la confidencialidad de la comunicación o esta haya sido hecha de forma anónima, se enviará un acuse de recibo al informante.

5. Comunicación con el informante.

En caso de que resulte necesario, se podrá mantener comunicación con el informante (si éste se identificó) y se podrá solicitar información adicional.

6. Derechos de la persona afectada.

Toda persona afectada por la información recibida tiene derecho a que se le informe de las acciones u omisiones que se le atribuyen, y a ser oída en cualquier momento. Dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.

Asimismo, se garantiza el respeto a la presunción de inocencia y al honor de las personas afectadas y a sus derechos en materia de protección de datos personales.

7. Confidencialidad.

Se garantiza en todo momento la confidencialidad cuando la comunicación sea remitida por canales que no sean los establecidos o a miembros del personal no responsable de su tratamiento, al que se habrá formado en esta materia y advertido de la tipificación como infracción muy grave de su quebranto y, asimismo, el establecimiento de la obligación del receptor de la comunicación de remitirla inmediatamente al Responsable del Sistema.

8. Determinación del plazo máximo para dar respuesta a las actuaciones de investigación.

El plazo de respuesta al informante no podrá ser superior a tres meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante, a tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, este podrá extenderse hasta un máximo de otros tres meses adicionales.

9. Clasificación.

El Responsable del Sistema Interno de Información analizará y clasificará la información, identificando varios escenarios:

10. Admisión, inadmisión y derivación a otros canales.

Una comunicación podrá ser inadmitida al considerar que no es pertinente, que es improcedente o no relacionada con las materias a comunicar a través del canal, siendo por tanto motivos de inadmisión:

a) Cuando los hechos relatados no sean verosímiles.

b) Cuando no sean constitutivos de infracción del ordenamiento jurídico.

c) Cuando la comunicación carezca de fundamento.

d) Cuando la información no contenga información nueva y significativa de otra comunicación anterior ya conclusa.

En este caso, se procederá a comunicar este extremo de forma motivada al informante y se procederá al archivo de la comunicación, pudiendo de forma adicional y si procediese, redirigir al informante al canal adecuado en el caso de que su información sí tuviese cabida en otros ámbitos de actuación.

Asimismo, información que pudiera resultar de interés para la gestión del sistema de calidad por informar acerca de posibles no conformidades con sus procedimientos y procesos podrá ser derivada al departamento correspondiente.

En caso de que la denuncia sea considerada pertinente, se procederá a remitir una comunicación al informante confirmando la apertura del expediente.

En ambos casos, como prueba de esta debida diligencia, tanto en la admisión como inadmisión, se dejarán debidamente documentados los motivos que han llevado a la decisión.

11. Comunicación al denunciado.

Salvo que ponga en riesgo el curso de la investigación, se informará al denunciado de la comunicación recibida, dándole traslado del contenido básico de la información recibida, así como dándole traslado igualmente de cuáles son sus derechos.

En caso de decidir no informar en un primer momento al denunciado se documentará esta decisión por escrito dejando constancia de los motivos por los que se ha optado por esta resolución.

12. Remisión al Ministerio Fiscal.

Se remitirá con carácter inmediato al Ministerio Fiscal la información recibida cuando los hechos pudieran ser indiciariamente constitutivos de delito.

En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

Si no estuviese claro desde el primer momento, se podrá esperar para tomar esta decisión a las conclusiones de la investigación interna.

B. Fase de investigación. Gestión pre-procesal.

Las pautas indicadas a continuación serán aplicables a aquellos casos en los que, sin existir un procedimiento judicial abierto, se ha tenido conocimiento de un hecho que puede ser constitutivo de delito.

1. Apertura de expediente de investigación.

Cuando se determine que los hechos suponen suficiente indicio que apunten a un posible incumplimiento, se abrirá el correspondiente expediente interno de investigación

El Responsable del Sistema interno será en principio el encargado de llevar a cabo la investigación, salvo que se detecte una situación de conflicto de intereses, en cuyo caso se pondrá en conocimiento del Compliance Officer que tomará la decisión de nombrar un responsable de la investigación alternativo, que podrá ser interno o externo.

Todas las áreas de la organización quedan obligadas a prestar la colaboración que resulte necesaria para que el Responsable pueda llevar a cabo la misma con todos los recursos que estime oportunos.

El Responsable abrirá el correspondiente expediente, que recogerá todas las incidencias que se produzcan en el desarrollo de su actuación, tendrá carácter reservado y se regirá por lo dispuesto en la normativa en materia de Protección de Datos de Carácter Personal y normativa de desarrollo.

Se emitirá un Informe previo con el siguiente contenido mínimo de manera que pueda servir como punto de partida para la investigación:

- Detalle de la comunicación, incluyendo fecha de recepción.
- Datos aportados en la comunicación, incluyendo cualquier documentación que se haya podido aportar.
- Una primera valoración del contenido de la comunicación y de la fiabilidad del informante (si se ha identificado).
- Análisis previo de la información apuntando las hipótesis más probables y las de mayor riesgo.
- Medidas cautelares que se propongan o se hayan llevado a cabo de forma urgente, en el caso de que el Responsable las haya considerado necesarias para garantizar sus actuaciones y la correcta marcha de la investigación interna, para evitar cualquier consecuencia negativa o para proteger a empleados (por ejemplo, la suspensión de empleo y sueldo de la persona involucrada).

En caso de que se considere que los hechos son de cierta gravedad siendo necesarias medidas urgentes de reacción o contención, este informe se trasladará a la alta dirección para que tenga conocimiento de esta información y, si procede, pueda tomar una decisión en relación con las medidas propuestas.

Igualmente, se pondrá a disposición del denunciado de los hechos, un análisis previo de las pruebas aportadas con el fin de que pueda alegar lo que estime oportuno en su defensa, salvo que en este primer momento se determine que no es oportuna la comunicación para no entorpecer la investigación o evitar la destrucción de pruebas.

2. La investigación interna.

En la investigación podrán participar aquellas personas que determine el Responsable en función de las circunstancias concretas de cada caso.

La Función de Compliance, con apoyo del Órgano de Gobierno, garantizará que la investigación disponga de todos los medios necesarios y que para la misma se tenga acceso a toda la información y documentación, así como las personas que pudieran tener relación con el caso.

Se podrá considerar externalizar la investigación con expertos externos en caso de que la Dirección, el Compliance Officer o miembros del Órgano de Gobierno u otros puestos relevantes se vean afectados por los hechos investigados o cuando ya desde un primer examen se considere que la investigación va a resultar compleja.

Esta decisión será tomada por el Compliance Officer que lidere la investigación, poniendo en conocimiento de esta necesidad al Órgano de Gobierno junto con la motivación de dicha decisión.

En caso de externalización, será indispensable que el experto externo informe en todo momento de la marcha de la investigación a la Función de Compliance, de manera que disponga en todo momento de la información necesaria para realizar el seguimiento.

Los expertos externos deben garantizar en todo caso el cumplimiento de la normativa de protección de datos, la confidencialidad y el secreto de las comunicaciones. Este externo debe suscribir un contrato de encargo de tratamiento en los términos del artículo 28 del RGPD.

Se podrá hacer uso de todos los medios jurídicamente válidos, incluyendo, entre otros, entrevistas, el examen de la documentación de cualquier tipo y en cualquier soporte que se entienda que puede ser de utilidad para la investigación, la recuperación y el análisis de la información contenida en soportes informáticos mediante el uso de herramientas de software y hardware que preserven la integridad de la evidencia y la posibilidad de aportarla como medio de prueba a un procedimiento penal.

Sólo el Compliance Officer será el competente para autorizar o decidir sobre la colaboración de asesores o colaboradores expertos externos en la investigación o en las sesiones que celebre el propio órgano, para lo cual ponderará la gravedad de los presuntos hechos u otros motivos, como la conveniencia de una mayor objetividad e imparcialidad de la investigación cuando la actuación de la Función de Compliance y Antisoborno tenga su origen en el anuncio de la presentación de una querella o de una denuncia.

Será igualmente competencia de Órgano de Compliance autorizar la asistencia de notarios cuando se considere conveniente para asegurar la validez de las pruebas a obtener en el marco de la investigación interna.

3. Conclusiones.

Una vez finalizada la investigación interna en los plazos establecidos se elaborará un informe con las conclusiones de esta y con propuestas de actuación motivadas.

En caso de que la investigación haya sido hecha por un experto externo será responsabilidad de éste la elaboración del Informe y su presentación ante el Responsable del Sistema Interno y el Compliance Officer.

El informe deberá ofrecer como mínimo el siguiente contenido, de manera que quede la investigación debidamente documentada y sea la base de la toma de decisiones posteriores:

- Aspectos técnicos: Título, autor, fecha, finalidad, origen, nivel de confidencialidad.
- Antecedentes y contexto del caso y personas o departamentos objeto de investigación.
- o, una relación circunstanciada de hechos, si se hubieran detectado hechos relevantes, las actuaciones realizadas con el fin de esclarecer los hechos y la valoración de las pruebas practicadas y de los indicios obtenidos.
- Objeto de la investigación y su finalidad.
- Actuaciones y aspectos analizados, indicando los hechos relevantes investigados y detectados.
- Relación de toda la documentación analizada y utilizada.
- Circunstancias que hayan podido limitar la actuación de la investigación.
- Conclusiones.
- Propuesta de medidas a adoptar.
- En caso de proponer medidas disciplinarias, graduación de las infracciones, de acuerdo con la legislación laboral y el convenio colectivo vigente.

4. Adopción y toma de decisiones en base a las conclusiones.

De forma que se evidencie la imparcialidad e independencia del proceso de investigación, la decisión final sobre las medidas propuestas en el Informe de Investigación se tomará por la Alta Dirección, es decir, por aquellas personas con los más altos niveles de responsabilidad en la organización.

De esta manera igualmente quedará evidencia de su participación y compromiso con el proceso.

En caso de detectarse un posible conflicto de intereses en los miembros del órgano decisorio por afectar a su área de responsabilidad o por cualquier circunstancia que pueda poner en peligro su objetividad o su imparcialidad se habrá de abstener de participar en la toma de decisión poniéndolo en conocimiento del Compliance Officer para que se determine una alternativa.

Entre las decisiones que se pueden adoptar se encuentran las sanciones disciplinarias a los empleados afectados, que serán establecidas en función de la gravedad de los hechos y aplicando la graduación y consecuencias contempladas en Convenio o Estatuto de Trabajadores. Cuando se determinen consecuencias disciplinarias, habrán de ser supervisadas por las personas competentes, en concreto el Departamento de RRHH.

En caso de que el investigado sea un tercero como, por ejemplo, un proveedor, cliente o socio de negocio, las medidas se limitarán al ámbito mercantil, por ejemplo, la limitación de actuaciones, la diligencia reforzada o, en casos graves, la rescisión unilateral de relación contractual por parte de la organización.

5. Seguimiento de las decisiones adoptadas.

Tras la finalización del proceso de investigación y una vez efectuada la toma de decisiones que se estimen oportunas, el Responsable del Sistema Interno de Información hará un seguimiento de que las decisiones adoptadas se llevan a cabo debidamente.

Dicho seguimiento tiene como finalidad comprobar que las medidas adoptadas se aplican, contribuyendo así a la mejora continua del modelo de gestión de riesgos de la organización, y a reforzar la cultura de Compliance Penal.

C. Actuación procesal.

Las pautas indicadas a continuación serán aplicables en aquellos casos en los que la organización se encuentre o es inminente que se encuentre investigada en un procedimiento penal.

En los casos en los que exista una resolución judicial que adopte contra la organización diligencias antes de que se le cite formalmente en el domicilio social de acuerdo con el procedimiento establecido en los arts. 119 y 120

LECrim., el Compliance Officer deberá ser convocado por el Órgano de Gobierno de forma urgente.

Salvo conflicto de intereses, el Compliance Officer será el órgano encargado de gestionar las líneas básicas de estrategia procesal, así como de todas las estrategias corporativas de reacción al procedimiento penal.

Una vez se tenga conocimiento de procedimiento penal, el Compliance Officer llevará a cabo las pautas definidas en el apartado anterior relativas a la Investigación interna.

En todo caso, las actuaciones que se realicen estarán orientadas por el principio de vocación de cumplimiento de la legalidad de acuerdo con las exigencias que el ordenamiento jurídico-penal dirige a las personas jurídicas, colaborando la organización y todo su personal en todo momento con las autoridades correspondientes de cara a un mejor esclarecimiento de los hechos y determinación de posibles responsabilidades penales. Todo ello sin perjuicio de las decisiones disciplinarias previstas.

Designación del representante procesal.

La organización, de acuerdo con lo dispuesto en los arts. 119 y 120 LECrim., designará en su momento, como representante procesal en el procedimiento, a la persona que considere tiene mejor conocimiento en materia de prevención de delitos.

También designará al abogado defensor y procurador de la entidad.

Se podrá permitir al abogado defensor que participe en las sesiones del Compliance Officer, con voz, pero sin derecho a participar en las votaciones.

De acuerdo con la propia evolución del procedimiento penal, la organización podrá modificar la persona que actúa como representante procesal de la misma, si fuese la opción más conveniente.

Nunca podrá ser designado representante procesal de la organización una persona que pueda tener conflictos de intereses procesales con la entidad, bien porque se encuentre ya investigada en el mismo procedimiento o porque existe la posibilidad de pueda ser investigada en el futuro o que resulte ser el representante procesal de la/s persona/s física/s presuntamente implicada/s en los hechos.

XIV. RESOLUCIÓN DE CONSULTAS

El canal interno podrá ser igualmente utilizado como fuente interna de recepción de consultas y dudas en materia de cumplimiento normativo.

La resolución de las dudas generales planteadas será resuelta por en un plazo no superior a 1 mes.

En el caso de que se detecte una incidencia importante o significativa en cuanto a volumen de consultas acerca de un tema en concreto el Responsable del Sistema Interno de Información, o en su caso el Compliance Officer, podrá recomendar acciones de concienciación o formación para

reforzar el conocimiento y los riesgos penales que afectan a la actividad en general.

El Responsable del Sistema Interno de Información mantendrá un repositorio de preguntas frecuentes que permita enriquecer su sistema en materia de cumplimiento penal.

XV. PUBLICIDAD Y REGISTRO DE INFORMACIONES.

A. Información.

Se proporcionará a los interesados información adecuada, de forma clara y fácilmente accesible, sobre el Sistema Interno de Información y el uso del canal, así como sobre los principios esenciales de este procedimiento de gestión, incluidos con ese propósito en la Política del Sistema Interno de Información.

Al contar con página web, esta información constará en la página de inicio del canal, en una sección separada y fácilmente identificable.

B. Registro de Informaciones.

La organización cuenta con un libro-registro para recopilar las informaciones recibidas y del detalle de las investigaciones internas a que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad y protección de datos personales.

Este registro no será público y 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 al contenido del referido registro.

Los datos personales relativos a las informaciones recibidas y a las investigaciones internas solo se conservarán durante el período que sea necesario y proporcionado y, en ningún caso podrán conservarse los datos por un período superior a diez años.

El Responsable del Sistema Interno de Información será el encargado de llevar el libro registro y de su custodia. Se archivará junto con los expedientes de investigación abiertos, aplicando medidas de seguridad de alto nivel, con llave tanto en los armarios como en la puerta de acceso en caso de archivo físico y con contraseña de acceso en caso de archivo digital.

Los expedientes se archivarán en orden cronológico, por fecha de entrada.

XVI. DOCUMENTACIÓN Y SISTEMA DE ARCHIVO DE LAS ACTUACIONES.

Toda la información generada por las comunicaciones será conservada en los sistemas y con las medidas de seguridad establecidas en el marco de su sistema de gestión de protección de datos, durante los plazos de conservación que se pudieran determinar internamente ene aplicación de los principios aplicables en materia de protección de datos de carácter personal o durante

los plazos de los que, de acuerdo con la ley, pudieran derivarse responsabilidades como consecuencia de las actuaciones investigadas.

A continuación, se establecen los plazos de conservación en función de la clasificación de las comunicaciones recibidas, incluyendo la necesidad de mantenerla de forma anonimizada en los sistemas una vez que el tratamiento de los datos personales que pudieran incluir dichas comunicaciones deje de resultar pertinente.

Asimismo, en el caso de que la información se haya de conservar durante plazos amplios de tiempo se podrá valorar la posibilidad de mantener la información bloqueada y únicamente accesible para el Responsable del Sistema Interno de Información y el Compliance Officer.

Clasificación		**Plazo de conservación**	**Anonimización de los datos personales**	**Necesidad de bloqueo**
Consultas		Indefinido, como repositorio de conocimientos	SI (la identificación del remitente no se considera relevante)	N/A
No admisión		3 meses (salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema)	SI (Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada)	N/A
Derivación a otros Canales		3 meses		
Expedientes de investigación	Investigación archivada sin consecuencias	3 meses una vez cerrado el expediente	No procede (la identificación de los interesados es relevante e indispensable)	SI
	Investigación con identificación de un posible incumplimiento o ilícito	Mientras puedan derivarse responsabilidades personales o de la compañía. En ningún caso nunca por un plazo superior a diez años.	No procede (la identificación de los interesados es relevante e indispensable)	SI

XVII. PROTECCIÓN DE DATOS PERSONALES.

A. Régimen jurídico del tratamiento de los datos personales y licitud del tratamiento.

Los tratamientos de datos personales que deriven de la gestión de estas comunicaciones se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), en la Ley

Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales(LOPDGDD), 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 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.

La base de legitimación del tratamiento de datos personales en este marco se regirá por los siguientes preceptos:

- ✓ Es lícita la creación y mantenimiento de un sistema de información a través del cual pueda ponerse en conocimiento de la Organización, incluso anónimamente, la comisión en su seno o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable.
- ✓ Es lícito el tratamiento de datos necesario para garantizar la protección de las personas que informen sobre infracciones normativas. Se podrán tratar datos con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- ✓ El tratamiento de datos en canales internos se realizará en virtud de obligación legal del artículo 6.1.c del RGPD cuando la organización venga a estar obligada por la Ley 2/2023 a habilitar un Sistema Interno de Información.
- ✓ Si no fuera obligatorio, se presume amparado en el interés legítimo del artículo 6.1.e del RGPD. El tratamiento de las categorías especiales de datos personales por razones de un interés público esencial se podrá realizar conforme a lo previsto en el artículo 9.2.g) del RGPD.

B. Deber de Información y ejercicio de derechos

- ✓ Los empleados y terceros deberán ser informados acerca de la existencia de estos sistemas de información.
- ✓ La persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante.
- ✓ Los interesados podrán ejercer los derechos a que se refieren los artículos 15 a 22 del RGPD, a través del canal de protección de datos de la Organización.
- ✓ En caso de que la persona a la que se refieran los hechos relatados en la comunicación ejerciese el derecho de oposición, se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales.

C. Acceso a los datos.

El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a:

- ✓ El Responsable del Sistema y a quien lo gestione directamente.
- ✓ El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de

medidas disciplinarias contra un trabajador. En el caso de los empleados públicos, el órgano competente para la tramitación del mismo.

- ✓ 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.
- ✓ Los encargados del tratamiento que eventualmente se designen.
- ✓ El delegado de protección de datos.

No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.

Sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador, dicho acceso se permitirá al personal con funciones de gestión y control de recursos humanos.

Deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.

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.

Se suprimirán todos aquellos datos que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en la Ley 2/2023 / en el alcance.

Los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

Una vez acreditada la existencia de información no veraz, esta se suprimirá inmediatamente, salvo que dicha veracidad pueda suponer un ilícito penal, en cuyo caso podrá ser conservada mientras se tramita el proceso judicial.

Si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de estos, salvo que dicha información fuera parte esencial del motivo de la denuncia.

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 Interno de Información.

Las denuncias 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 32 de la LOPDGDD.

Transcurrido el plazo mencionado en el párrafo anterior, los datos podrán seguir siendo tratados, por el órgano al que corresponda la investigación de los hechos denunciados, no conservándose en el propio Sistema Interno de Información.

Los empleados y terceros deberán ser informados acerca del tratamiento de datos personales en el marco del Sistema Interno de Información.

D. Preservación de la identidad del informante.

Se habrá de tener en cuenta:

- ✓ Quien presente una comunicación o lleve a cabo una revelación pública tiene derecho a que su identidad no sea revelada a terceras personas.
- ✓ No se obtendrán datos que permitan la identificación del informante. El Sistema y en especial el canal habilitado dispondrán de medidas de seguridad técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado.
- ✓ La identidad del informante solo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.

El Responsable del Sistema Interno de Información habrá de velar por que se cumplan estos requisitos.