

CLASIFICACIÓN

POLÍTICA INTERNA DE LA COMPAÑÍA

PROCEDIMIENTO DE GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN

TODOS LOS DERECHOS RESERVADOS. NO SE PERMITE SIN AUTORIZACIÓN ESCRITA DE EPICOM LA CESIÓN O REPRODUCCIÓN TOTAL O PARCIAL DE ESTE DOCUMENTO, NI EL USO Y COMUNICACIÓN DE SU CONTENIDO.

FECHA Y FIRMA	
REALIZADO POR: DPTO. RRHH	<i>A. Molina</i> <i>15-12-2024</i>
REVISADO POR: DPTO. CALIDAD y MA	<i>M. Jiménez</i> <i>15-12-2024</i>
APROBADO POR: CEO	<i>J.C del Peso</i> <i>15-12-2024</i>

REGISTRO DE EDICIONES Y MODIFICACIONES

ED.	FECHA	MODIFICACIÓN EFECTUADA (Indicar capítulos o apartados modificados y una breve descripción)	REALIZADO POR	NOTA DE CAMBIO
1	15/12/24	Se edita nuevo	RRHH	N/A

N/P = NO PROCEDE

ÍNDICE

1. OBJETO	4
2. ÁMBITO DE APLICACIÓN	6
2.1. ÁMBITO SUBJETIVO	6
2.2. ÁMBITO OBJETIVO.....	6
3. DOCUMENTOS Y NORMAS APLICABLES	8
3.1. REFERENCIAS GENERALES.....	8
3.2. REFERENCIAS ESPECÍFICAS.....	8
4. PROTECCIÓN DE DATOS	9
5. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN	11
5.1. RECURSOS DOCUMENTALES Y REGISTROS	11
6. OBLIGACIONES EN RELACIÓN CON EL PRESENTE PROCEDIMIENTO	12
6.1. INCUMPLIMIENTO DEL PROCEDIMIENTO	13
7. PROTECCIÓN DE INFORMANTES Y PERSONAS AFECTADAS.....	14
7.1. PRESERVACIÓN DE LA IDENTIDAD DEL INFORMANTE Y DE LAS PERSONAS AFECTADAS.....	14
7.2. CONDICIONES DE PROTECCIÓN.....	14
7.3. PROHIBICIÓN DE REPRESALIAS Y MEDIDAS DE PROTECCIÓN FRENTE A ELLAS.	15
7.4. SUPUESTOS DE EXENCIÓN Y ATENUACIÓN DE LA SANCIÓN	16
8. VIAS PARA COMUNICAR INFRACCIONES NORMATIVAS	18
9. TRAMITACIÓN DE LAS COMUNICACIONES	19
9.1. FASE DE FORMULACIÓN DE LA COMUNICACIÓN	19
9.2. ACCESO AL SISTEMA INTERNO DE INFORMACIÓN.....	20
9.3. OBLIGACIONES DEL INFORMANTE	21
9.4. TRÁMITE DE ADMISIÓN O INADMISIÓN	21
9.4.1. Inadmisión.....	22
9.4.2. Admitir a trámite la comunicación	22
9.5. DILIGENCIAS DE INVESTIGACIÓN	23
9.6. TERMINACIÓN DE ACTUACIONES	24
10. REVISIÓN Y SEGUIMIENTO	26

1. OBJETO

El objeto del Procedimiento de Gestión del Sistema Interno de Información (en adelante, el Procedimiento), es establecer las previsiones necesarias para gestionar el Sistema Interno de Información de EPICOM conforme a 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.

La presente Ley tiene por finalidad otorgar una protección adecuada frente a las represalias que puedan sufrir las personas físicas que informen sobre alguna de las acciones u omisiones a que se refiere el artículo 2 de la Ley 2/2023, de 20 de febrero, a través de los procedimientos previstos en la misma.

La Gestión del Sistema Interno de Información regula la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción conforme a:

1. La gestión del Sistema Interno de Información se podrá llevar a cabo dentro de la propia entidad u organismo o acudiendo a un tercero externo, en los términos previstos en esta ley. A estos efectos, se considera gestión del Sistema la recepción de informaciones.

2. La gestión del sistema por un tercero externo exigirá en todo caso que este ofrezca garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones.

3. La gestión del Sistema Interno de Información por un tercero no podrá suponer un menoscabo de las garantías y requisitos que para dicho sistema establece esta ley ni una atribución de la responsabilidad sobre el mismo en persona distinta del Responsable del Sistema previsto en el artículo 8.

4. El tercero externo que gestione el Sistema tendrá la consideración de encargado del tratamiento a efectos de la legislación sobre protección de datos personales. El tratamiento se registrará por el acto o contrato al que se refiere el artículo 28.3 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

En EPICOM se rige por los estándares mas altos de transparencia, honestidad y responsabilidad.

También, el presente Sistema Interno de Información, en adelante Sistema, tiene como finalidad el fortalecimiento de la cultura de la información, de las infraestructuras de integridad de las organizaciones y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público.

Mediante este Procedimiento pretendemos explicar a los Miembros de EPICOM, que pueden y deben informar sobre actividades ilícitas sin temor a ser perseguidos, discriminados o a sufrir algún otro tipo de represalia.

A tal efecto, se ha habilitado un Sistema de comunicación para que, ante la certeza o sospecha fundada de que se esté cometiendo una conducta ilícita en el seno EPICOM, relacionada con actuaciones con relevancia penal o que infrinjan el Código Ético de la Entidad o el Derecho de la Unión Europea, trasladen de forma confidencial dicha comunicación al objeto de que sea investigada, constituyendo un medio eficaz para prevenir y luchar contra dichas conductas y anticipar o mitigar sus consecuencias.

El Sistema Interno de Información incorpora mecanismos que garantizan la confidencialidad de todas las informaciones, y ofrece un espacio de comunicación seguro para mantener contacto con los órganos de cumplimiento de EPICOM y permite la interacción entre esta y los informantes de manera anónima, sin sufrir represalias de ninguna clase.

2. ÁMBITO DE APLICACIÓN

2.1. ÁMBITO SUBJETIVO

Este Procedimiento resulta de aplicación a todo el personal que preste sus servicios en EPICOM (personal laboral fijo o temporal), así como a las personas pertenecientes al órgano de administración de la entidad. Asimismo, será de aplicación a aquellas personas que presten sus servicios de manera habitual, aunque no formen parte de la plantilla (a través de contrata o de beca).

También resultará de aplicación a aquellas personas que comuniquen información sobre infracciones obtenida en el marco de una relación laboral ya finalizada, así como a aquellos cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección.

Adicionalmente, se incluye en el ámbito de aplicación a cualquier persona, física o jurídica, que haya obtenido información sobre infracciones normativas en un contexto profesional.

2.2. ÁMBITO OBJETIVO

A través del Sistema Interno de Información se podrán comunicar:

- Las infracciones del Derecho de la Unión Europea (UE) siempre que entren dentro del ámbito de aplicación de los actos de la UE enumerados en el anexo de la Directiva 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019 y que afecten a los intereses financieros de la UE o incidan en el mercado interior.
- En el ámbito del ordenamiento jurídico español las infracciones penales, las infracciones administrativas graves y muy graves y las infracciones del Derecho laboral en materia de seguridad y salud en el trabajo.
- Incumplimientos del Código Ético o del Protocolo de Integridad, en tanto que constituyen normas esenciales del Sistema de cumplimiento de EPICOM. La tramitación de las comunicaciones que se refieran a este tipo de incumplimientos no sujetos a la Ley 2/2023, se realizará a tenor de los principios generales establecidos en la Política del Sistema Interno de Información.

También aplicará a informantes que comuniquen o revelen públicamente información sobre infracciones que hubieran tenido lugar en el marco de una relación laboral o

estatutaria ya finalizada, voluntarios, becarios, trabajadores con periodos de formación con independencia de que perciban o no una remuneración, así como a aquellos cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenido durante el proceso de selección o de negociación precontractual.

3. DOCUMENTOS Y NORMAS APLICABLES

3.1. REFERENCIAS GENERALES

CÓDIGO	TÍTULO UNIFORME	TÍTULO DEL DOCUMENTO	ED	FECHA
EP100NGN00001	NORMA	Estructura Orgánica de la Empresa	*	*
EP100NGN00002	NORMA	Manual de Gestión de Calidad y Medio Ambiente	*	*

*Se aplica la última en vigor.

3.2. REFERENCIAS ESPECÍFICAS

N/A

4. PROTECCIÓN DE DATOS

Los tratamientos de datos personales que deriven de la aplicación de esta ley se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales 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 el presente título.

El responsable del tratamiento de los datos personales tratados en el Sistema Interno de Información recaerá sobre la persona el responsable del mismo Sistema.

Los datos de carácter personal y demás información que, en su caso, se facilite a través del Sistema Interno de Información serán tratados con la finalidad de recibir comunicaciones de infracciones normativas, analizar su contenido y gestionar el expediente correspondiente. El tratamiento de los datos personales está basado en el cumplimiento de una obligación legal, de conformidad con el artículo 30 de la Ley 2/2023.

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

Los interesados podrán ejercer los derechos de acceso, rectificación, supresión, portabilidad y la litación u oposición dirigiéndose por escrito a través de la dirección de correo electrónico: canalinterno@epicom.es.

En ningún caso los datos personales relativos a las informaciones recibidas y a las investigaciones internas podrán conservarse por un periodo superior a diez años.

El acceso a los datos personales contenidos en el Sistema Interno de Información (art. 32 de la Ley 2/2023, de 20 de febrero) quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente a:

- El Responsable del Sistema y a quien lo gestione directamente.
- El responsable de recursos humanos, cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.
- El responsable de los servicios jurídicos de EPICOM, 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, en su caso.

Por otro lado, la identidad del informante sólo podrá ser comunicada (art. 33 de la Ley 2/2023, de 20 de febrero) a la autoridad judicial, al ministerio fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.

5. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN

El órgano de administración u órgano de gobierno de cada entidad u organismo obligado por esta ley será el competente para la designación de la persona física responsable de la gestión de dicho sistema o «Responsable del Sistema», y de su destitución o cese.

Si se optase por que el Responsable del Sistema fuese un órgano colegiado, este deberá 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 de la persona física individualmente designada, así como de las integrantes del órgano colegiado deberán ser notificados a la Autoridad Independiente de Protección del Informante, A.A.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 del Sistema deberá desarrollar sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad u organismo, 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.

El Responsable del Sistema designará a un suplente para los supuestos de ausencia, enfermedad, vacancia o conflictos de interés, que en su caso será el CEO de EPICOM

Asimismo, se designará una segunda persona responsable, que igualmente recibirá los informes de viabilidad de las comunicaciones, en aras de evitar una eventual mala praxis en la tramitación de las mismas. Esta segunda persona responsable será nombrada por la dirección de la empresa, limitándose a validar la correcta gestión de las comunicaciones.

5.1. RECURSOS DOCUMENTALES Y REGISTROS

La gestión de los registros se realizará de acuerdo con lo descrito en el “Plan General de la Documentación” (EP100PGN00001).

6. OBLIGACIONES EN RELACIÓN CON EL PRESENTE

PROCEDIMIENTO

Con carácter general, todo el personal de EPICOM, incluidas las personas pertenecientes al órgano de administración de la entidad, deberán guardar la más estricta confidencialidad acerca de:

- La identidad del informante
- La identidad de las personas afectadas por la comunicación
- La identidad de cualesquiera otras personas mencionadas en la comunicación
- Cualquier tipo de información comunicada a través del Sistema Interno de Información

En especial, las personas legitimadas para conocer la identidad del informante serán garantes de la confidencialidad de dicha identidad y la de cualquier tercero mencionado en la comunicación.

Cuando la comunicación sea remitida por vías distintas a las establecidas en el presente Procedimiento o a miembros del personal no responsables de su tratamiento, el receptor de la comunicación deberá remitirla inmediatamente a la persona Responsable del Sistema (en adelante, “el Responsable del Sistema”).

El Responsable del Sistema Interno de Información podrá solicitar al personal de EPICOM su colaboración en las diligencias de investigación, que tendrá, dentro del marco legal aplicable, la obligación de:

- Comparecer ante el Responsable del Sistema, en el caso de que así sean requeridos contestando a todas las preguntas que se les formule;
- Contestar a todos los requerimientos de información o documentación formulados por el Responsable del Sistema;
- Mantener confidencialidad sobre la existencia de la investigación y su contenido.
- La solicitud de colaboración deberá ser atendida sin dilación y, en todo caso, en los plazos señalados por el Responsable del Sistema Interno de Información.
- Asimismo, el personal de EPICOM, incluidas las personas pertenecientes al órgano de administración de la entidad, deberán abstenerse de:

1. Obstaculizar la presentación de comunicaciones.
2. Impedir, frustrar o ralentizar el seguimiento de las comunicaciones, incluyendo la aportación de información o documentación falsa o incompleta si fuesen requeridos para ello.
3. Adoptar cualquier represalia, incluidas las amenazas de represalia y las tentativas de represalia, contra las personas que presenten una comunicación o las demás personas incluidas en el ámbito de protección, conforme a lo establecido en el Anexo del presente Procedimiento.
4. Comunicar información a través del Sistema Interno de Información a sabiendas de su falsedad.

6.1. INCUMPLIMIENTO DEL PROCEDIMIENTO

Con carácter general, todo el personal de EPICOM, incluidas las personas pertenecientes al órgano de administración de la entidad, está obligado a cumplir con lo establecido en el presente Procedimiento, pudiendo proceder la adopción de medidas disciplinarias en caso de incumplimiento.

Adicionalmente, la Ley 2/2023 establece un régimen sancionador al que están sujetas todas las personas físicas y jurídicas que cometan alguna de las infracciones tipificadas en la citada ley. En el caso de que sean personas físicas las responsables de las infracciones, el importe de las multas oscilará entre 1.001 y 300.000 euros, dependiendo de si se ha cometido una infracción leve, grave o muy grave.

En el ámbito del sector público estatal, será competente para la aplicación del régimen sancionador la Autoridad Independiente de Protección del Informante (A.A.I.).

La obligación de cumplir con este Procedimiento se extiende a las personas ajenas a EPICOM que formulen una comunicación a través del Sistema Interno de Información de la entidad.

7. PROTECCIÓN DE INFORMANTES Y PERSONAS AFECTADAS

Las personas que comuniquen infracciones tendrán derecho a las medidas de protección establecidas en los artículos 35 y 36 de la Ley 2/2023, de 20 de febrero:

7.1. PRESERVACIÓN DE LA IDENTIDAD DEL INFORMANTE Y DE LAS PERSONAS AFECTADAS

Preservar su identidad, exceptuándose la comunicación que pudiera efectuarse a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.

7.2. CONDICIONES DE PROTECCIÓN

Las personas que comuniquen o revelen infracciones de las previstas en el ámbito material de aplicación tendrán derecho a protección siempre que concurren las circunstancias siguientes:

- 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 la ley.
- La comunicación o revelación se haya realizado conforme a los requerimientos previstos en la ley.

Quedan expresamente excluidos de la protección prevista en esta ley aquellas personas que comuniquen o revelen:

- Informaciones contenidas en comunicaciones que hayan sido inadmitidas por algún canal interno de información o por la Autoridad Independiente de Protección del Informante.
- 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.
- Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores.

- Informaciones que se refieran a acciones u omisiones no comprendidas en el artículo 2 de la Ley 2/2023, de 20 de febrero.

Las personas que hayan comunicado o revelado públicamente información sobre acciones u omisiones de forma anónima pero que posteriormente hayan sido identificadas y cumplan las condiciones previstas en la ley, tendrán derecho a la protección que la misma contiene.

En relación con las comunicaciones falsas, la Ley 2/2023 establece en su artículo 63 que comunicar o revelar públicamente información a sabiendas de su falsedad será constitutivo de una infracción muy grave.

7.3. PROHIBICIÓN DE REPRESALIAS Y MEDIDAS DE PROTECCIÓN FRENTE A ELLAS.

La política del Sistema Interno de Gestión establece el principio de protección del informante, prohibiendo expresamente cualquier acto de represalia, amenaza de represalia o tentativa de represalia contra la persona informante.

Se entiende 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. Tal y como contempla el artículo 36.3 de la Ley 2/2023, de 20 de febrero, "a título enunciativo" se consideran represalias las que adopten la forma de:

- Suspensión del contrato de trabajo, despido o extinción de la relación laboral o estatutaria, incluyendo la no renovación o la terminación anticipada de un contrato de trabajo temporal una vez superado el período de prueba, o terminación anticipada o anulación de contratos de bienes o servicios, imposición de cualquier medida disciplinaria, degradación o denegación de ascensos y cualquier otra modificación sustancial de las condiciones de trabajo y la 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; salvo que estas medidas se llevaran a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral o reguladora del estatuto del empleado público correspondiente, por circunstancias, hechos o infracciones acreditadas, y ajenas a la presentación de la comunicación.
- Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.

- Evaluación o referencias negativas respecto al desempeño laboral o profesional.
- Inclusión en listas negras o difusión de información en un determinado ámbito sectorial, que dificulten o impidan el acceso al empleo o la contratación de obras o servicios.
- Denegación o anulación de una licencia o permiso.
- Denegación de formación.
- Discriminación, o trato desfavorable o injusto.

Las medidas de protección del informante previstas en el título VII también se aplicarán, en su caso, específicamente a los representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante.

Las medidas de protección del informante previstas en el título VII también se aplicarán, en su caso, a:

- Personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso,
- Personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante, y
- 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. A estos efectos, se entiende que la participación en el capital o en los derechos de voto correspondientes a acciones o participaciones es significativa cuando, por su proporción, permite a la persona que la posea tener capacidad de influencia en la persona jurídica participada.

7.4. SUPUESTOS DE EXENCIÓN Y ATENUACIÓN DE LA SANCIÓN

Cuando una persona que hubiera participado en la comisión de la infracción administrativa objeto de la información sea la que informe de su existencia mediante la presentación de la información y siempre que la misma hubiera sido presentada con anterioridad a que hubiera sido notificada la incoación del procedimiento de investigación o sancionador, el órgano competente para resolver el procedimiento, mediante resolución motivada, podrá eximirle del cumplimiento de la sanción administrativa que le correspondiera siempre que resulten acreditados en el expediente los siguientes extremos:

- 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.
- Haber cooperado plena, continua y diligentemente a lo largo de todo el procedimiento de investigación.
- 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.
- Haber procedido a la reparación del daño causado que le sea imputable.

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.

Lo dispuesto en este artículo no será de aplicación a las infracciones establecidas en la Ley 15/2007, de 3 de julio, de Defensa de la Competencia.

8. VIAS PARA COMUNICAR INFRACCIONES NORMATIVAS

En la web corporativa de EPICOM (www.epicom.es) se encuentra disponible un enlace denominado “Canal Ético” que permitirá el acceso a una plataforma que prioriza la seguridad de los datos de nuestros usuarios. Todos los datos de un caso o denuncia que se almacenan en nuestra plataforma se cifran de extremo a extremo. Esto significa que, incluso si los datos se interceptaran de alguna manera, serían incomprensibles sin la clave de descryptación proporcionada exclusivamente al usuario que genera los casos o denuncias.

La información de los casos queda almacenada en nuestros sistemas siempre de forma encriptada. Nadie con acceso al sistema o BBDD pueda descryptar la información sin disponer de la clave correspondiente a cada caso.

Esta medida de seguridad garantiza que la información de nuestros usuarios esté resguardada de cualquier acceso no autorizado y cumple con los estándares de privacidad y protección de datos.

El Sistema Interno de Información será el medio empleado y facilitado por la Entidad con este fin, si bien eventualmente el informante podrá solicitar realizar esta comunicación verbalmente mediante reunión presencia de acuerdo con el artículo 7 de la Ley 2/2023, de 20 de febrero.

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

Para evitar que se haga un mal uso del Sistema Interno de Información, se aplican criterios estrictos para admitir las comunicaciones con la exigencia de responsabilidad civil, penal o administrativa a las personas que comuniquen hechos con abuso de derecho o vulnerando el principio de buena fe.

Adicionalmente, la comunicación se podrá dirigir a un canal externo habilitado y gestionado por la Autoridad Independiente de Protección del Informante (A.A.I.), ente de derecho público de ámbito estatal vinculado al Ministerio de Justicia.

9. TRAMITACIÓN DE LAS COMUNICACIONES

9.1. FASE DE FORMULACIÓN DE LA COMUNICACIÓN

El acceso a la parte de creación y consulta de casos se realiza a través de una URL (www.epicom.es).

La persona que decida formular una comunicación deberá facilitar con la misma la máxima información disponible sobre los hechos comunicados, debiendo incluir expresamente:

- El tipo de vínculo que el informante mantiene con EPICOM, de acuerdo con el apartado 2.1 de este Procedimiento.
- La fecha o fechas en que se hubieran cometido los hechos denunciados como infractores (aunque sea por aproximación).
- La/s persona/s que, en su caso, fueran responsables de dicha infracción;
- Una descripción completa y precisa de los hechos;
- Documentos, datos y demás fuentes de prueba o información que, en su caso, pudieran permitir la investigación de los hechos.

El Responsable del Sistema Interno de Información procederá a acusar recibo de la comunicación en el plazo de siete días naturales siguientes a su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.

Una vez realizada la evaluación inicial de la comunicación por razón de la materia, el Responsable del Sistema derivará la comunicación al gestor del expediente teniendo en cuenta que:

A través del botón de crear denuncia se accede al formulario de creación de una denuncia.

A continuación, se especifican los distintos campos disponibles. Tipo de Denuncia: Podrá seleccionarse “Anónimo” o “Confidencial”. En el caso de seleccionar el tipo anónimo, no será necesario indicar nombre ni ningún dato identificativo. En el caso de del tipo confidencial, se habilitará el campo “Nombre” para que el informante pueda cumplimentarlo con su nombre y apellidos.

- Una denuncia de tipo confidencial, se mostrará el texto “Su identidad sólo será conocida por aquellos que gestionen la denuncia de manera confidencial”. En cualquiera de los dos casos, el usuario deberá marcar el “check” para dar su conformidad sobre el tratamiento.
- Nombre: Este campo sólo podrá ser cumplimentado si el tipo de denuncia es confidencial.
- Adjuntar documentación: A través del botón de adjuntar documentación, el sistema abrirá el explorador de Windows para que el informante pueda adjuntar un documento o varios a la denuncia. El límite es de 2 MB.
- Grabar Audio: Con esta opción se permite al denunciante realizar una grabación de audio de voz para añadirla al caso. Cuando se pulsa el botón, se muestra un aviso sobre los requisitos para poder realizar la grabación, así como el funcionamiento de la distorsión de voz:
- Guardar: A través de este botón se da por finalizada la denuncia y se procede a guardarla.

9.2. ACCESO AL SISTEMA INTERNO DE INFORMACIÓN

Los envíos de las comunicaciones sobre incidencias, infracciones o incumplimientos de las que se tengan conocimiento deberán ser cursados a través del Sistema Interno de Información, siendo dirigidos, en primer lugar, a los encargados de la gestión para la recepción de las informaciones sobre infracciones, que podrán actuar para realizar un primer análisis de la comunicación, su valoración y estudio sobre un posible conflicto de intereses de algún miembro Responsable del Sistema Interno de Información de EPICOM.

El responsable encargado del Sistema Interno de Información en EPICOM, será una persona directiva de EPICOM, que ejercerá su cargo con independencia del órgano de administración o de gobierno de la misma.

El mismo responsable del Sistema mandará acuse de recibo de la comunicación al informante, en el plazo de siete días naturales siguientes a su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.

En el caso de que el Responsable del Sistema persona física o la entidad en quien el órgano colegiado responsable haya delegado sus funciones, será un directivo de la entidad, que ejercerá su cargo con independencia del órgano de administración o de gobierno de la misma

El Sistema Interno de Información se encontrará alojado en la página web de EPICOM, en una sección separada, de forma clara y fácilmente accesible denominada “Canal Ético”.

9.3. OBLIGACIONES DEL INFORMANTE

- Describir de la manera más detallada posible las circunstancias que faciliten la identificación de la irregularidad.
- Proporcionar toda la documentación disponible acerca de la situación que se comunica, o indicios objetivos para poder obtener pruebas por parte del personal a quien se asigne la investigación sobre los hechos o comportamientos informados.
- Buena fe y diligencia: el informante deberá garantizar que la comunicación interna se formula actuando de buena fe, esto es, que crea que es sustancialmente cierta, que no sea infundada ni haga acusaciones falsas, ni que carezca de motivación o busque venganza o beneficio personal.
- No se admitirán comunicaciones basadas en opiniones que no vengán acompañadas de la suficiente fundamentación o evidencias ni aquellas otras que sean notoriamente falsas.
- Deber de confidencialidad: el informante bajo ningún concepto comunicará ni el contenido de la comunicación interna ni la identidad de las personas afectadas por la misma a terceros u otras unidades organizativas de EPICOM distintas de los Gestores del Sistema o del Responsable del Sistema Interno de Información y personal asignado a este.

Contravenir y romper esta obligación de confidencialidad podrá conllevar la adopción de distintas medidas: disciplinarias, según lo que dicte el régimen sancionador que resulte aplicable; contractuales, especialmente si el informante es o pertenece a un proveedor; e, incluso, el emprendimiento de acciones legales.

9.4. TRÁMITE DE ADMISIÓN O INADMISIÓN

Una vez analizada la comunicación, el gestor del expediente decidirá:

9.4.1. Inadmisión

- Cuando los hechos relatados carezcan de toda verosimilitud.
- Cuando los hechos relatados no sean constitutivos de infracción incluida en el ámbito de aplicación de este Procedimiento.
- Cuando la comunicación carezca manifiestamente de fundamento por no reunir los requisitos expresados en el apartado 6.1 de este Procedimiento o cuando existan indicios racionales de que la prueba se hubiera obtenido mediante la comisión de un delito;
- Cuando la comunicación no contenga información nueva y significativa sobre infracciones en comparación con una comunicación anterior respecto de la cual han concluido los correspondientes procedimientos, a menos que se den nuevas circunstancias que justifiquen un seguimiento distinto.

La inadmisión se comunicará al informante dentro de los cinco días hábiles siguientes, salvo que la comunicación fuera anónima o el informante hubiera renunciado a recibir comunicaciones de la Autoridad Independiente de Protección del Informante (A.A.I.).

9.4.2. Admitir a trámite la comunicación

Desplegando efectos, cuando proceda, el régimen de protección frente a posibles represalias en los términos previstos en el Anexo del presente Procedimiento.

- Admitir a trámite la comunicación. La admisión a trámite se comunicará al informante dentro de los cinco días hábiles siguientes, salvo que la comunicación fuera anónima o el informante hubiera renunciado a recibir comunicaciones de la Autoridad Independiente de Protección del Informante (A.A.I.).
- Remitir con carácter inmediato la información al Ministerio Fiscal cuando los hechos pudieran ser indiciariamente constitutivos de delito o a la Fiscalía Europea en el caso de que los hechos afecten a los intereses financieros de la Unión Europea.
- Remitir la comunicación a la autoridad, entidad u organismo que se considere competente para su tramitación.

En los casos de comunicaciones formuladas por personas que no estén incluidas en el ámbito subjetivo del presente Procedimiento, se procederá a inadmitir la comunicación sin perjuicio de darle el curso legal que proceda.

Con el fin de decidir sobre su admisión a trámite, se podrá solicitar al informante la aclaración o complemento de los hechos comunicados, aportando aquella documentación que pudiera ser necesaria para acreditar la existencia de la infracción normativa.

La decisión de admisión o inadmisión a trámite se comunicará al informante a la mayor brevedad posible. La comunicación de inadmisión a trámite se motivará de forma sucinta.

9.5. DILIGENCIAS DE INVESTIGACIÓN

El Responsable del expediente practicará todas las diligencias de investigación que estime oportunas para comprobar la veracidad de los hechos relatados, además evaluará si la denuncia está suficientemente documentada y si cumple con los requisitos para ser investigada.

- Realizar entrevistas con el informante, con las personas mencionadas en la comunicación o con personal de EPICOM, que deberán ser documentadas adecuadamente.
- Recabar toda la información o documentación que estime necesaria a cualesquiera de las Direcciones de la entidad.

Acceder a los sistemas informáticos y dispositivos que la entidad pone a disposición de sus empleados para fines profesionales (por ejemplo, ordenadores portátiles, cuentas de correo electrónico, dispositivos de almacenamiento, etc.), dentro de los límites establecidos en la normativa laboral y la normativa de protección de datos que resulte de aplicación.

Si fuera preciso, el gestor del expediente podrá contar con el auxilio necesario para la práctica de las diligencias de investigación que, en todo caso, deberá respetar los principios establecidos en la Política del Sistema Interno de Información. Los procedimientos de contratación que se deban seguir se llevarán a cabo con la celeridad necesaria que demande el cumplimiento de los plazos de la investigación.

La persona afectada por la comunicación será informada de los hechos que se le atribuyen, si bien esta información se proporcionará en el momento y en la forma que se consideren adecuados para garantizar el buen fin de la investigación. En ningún caso se le comunicará la identidad del informante ni tendrá acceso a la comunicación. Asimismo, tendrá derecho a ser oída en cualquier momento con el objeto de exponer su versión de los hechos y aportar aquellos medios de prueba que considere adecuados y pertinentes,

siempre con absoluto respeto a la presunción de inocencia. Se le deberá informar de la posibilidad de comparecer asistido por un abogado.

9.6. TERMINACIÓN DE ACTUACIONES

Concluidas las diligencias de investigación, el gestor del expediente emitirá un informe que contendrá un resumen de las diligencias practicadas con el fin de comprobar la verosimilitud de los hechos, la valoración de las mismas y las conclusiones alcanzadas.

El gestor del expediente procederá a archivar el expediente en los siguientes supuestos:

- Inexistencia de los hechos que pudieran constituir una infracción normativa incluida en el ámbito de aplicación de este Procedimiento.
- Cuando las diligencias practicadas no acrediten suficientemente la comisión de la infracción.
- Cuando los hechos probados no constituyan, de modo manifiesto, una infracción normativa incluida en el ámbito de aplicación de este Procedimiento.
- Cuando no se haya podido identificar a la persona o personas responsables.
- Cuando se concluyera, en cualquier momento, que ha prescrito la infracción.

No obstante, si la investigación pusiera de manifiesto alguna deficiencia a subsanar, se elaborará un informe con propuestas de mejora que se trasladará a Presidencia.

Es importante que la resolución sea clara, equitativa y acorde con las políticas establecidas.

El archivo del expediente será notificado al informante y, en su caso, a la persona afectada.

Si el gestor del expediente estima que las diligencias practicadas acreditan suficientemente la comisión de una infracción normativa incluida en el ámbito de aplicación de este Procedimiento, trasladará su informe a la persona titular de la Secretaría del Consejo y Dirección de Asuntos Jurídicos para que se pronuncie sobre la calificación jurídica de los hechos.

Recibido el informe jurídico, si los hechos pudieran revestir carácter delictivo se deberá informar de forma inmediata al Ministerio Fiscal o a la Fiscalía Europea en el caso de que los hechos afecten a los intereses financieros de la Unión Europea.

Asimismo, el gestor del expediente deberá proponer las medidas preventivas adecuadas para mitigar el riesgo de reiteración en la conducta infractora. En el caso de que la conducta infractora no hubiera cesado, también deberá elaborar una propuesta sobre la forma de restaurar la situación.

El plazo para finalizar las actuaciones y dar respuesta al informante no podrá ser superior a tres meses a contar desde la recepción de la comunicación completa o, en su caso, desde la subsanación de los requisitos que hubieran determinado la inadmisión de la comunicación. De forma motivada, este plazo podrá extenderse hasta un máximo de otros tres meses adicionales en casos de especial complejidad.

El informante y la/s persona/s a la/s que se refiere la comunicación podrán formular alegaciones en relación con las decisiones adoptadas por el gestor del expediente, quedando este habilitado para revisarlas si considera que existen motivos para ello.

10. REVISIÓN Y SEGUIMIENTO

Se revisará anualmente el presente Procedimiento y comunicará sus eventuales cambios o actualizaciones a los Miembros de EPICOM. Siempre y cuando la revisión y actualización se acometa bajo las circunstancias que a continuación se exponen a título enunciativo, pero no limitativo:

- Cambios en el Marco normativo vigente.
- Recomendaciones de la Autoridad Independiente de Protección del Informante u otras autoridades administrativas u órganos supervisores cuya actividad tenga incidencia en las cuestiones reguladas por el presente Procedimiento.
- Modificación de la estructura organizativa con vinculación a este Procedimiento, así como de los órganos de cumplimiento normativo y de los miembros del Comité.
- Modificaciones sustantivas en procedimientos vinculados.
- Cuando el resultado de su seguimiento y control aconseje modificar actuaciones para incrementar el grado de cumplimiento o mejorar su impacto en EPICOM o sus empleados y partes interesadas.