



TeleMadrid

**POLÍTICA DEL
SISTEMA
INTERNO DE
INFORMACIÓN**



ÍNDICE

I.	FINALIDAD Y OBJETO	2
II.	ALCANCE	2
III.	PRINCIPIOS QUE RIGEN EL CANAL.....	2
3.1.	Accesibilidad	3
3.2.	Buena fe.....	3
3.3.	Confidencialidad	3
3.4.	Objetividad e imparcialidad.....	3
3.5.	Transparencia	3
3.6.	Autoridad, independencia y conflicto de intereses.....	3
3.7.	Prohibición de represalias.....	3
IV.	CONDUCTAS QUE SE PUEDEN COMUNICAR.....	4
4.1.	Garantías del informante.....	5
4.2.	Garantías del posible implicado	5
V.	PRINCIPIOS ESENCIALES DEL PROCEDIMIENTO DE GESTIÓN DE LAS COMUNICACIONES	5
5.1.	Principios rectores del procedimiento	5
5.2.	Envío de acuse de recibo de la comunicación al informante	6
5.3.	Comunicación con el informante.....	6
5.4.	Determinación del plazo máximo para dar respuesta a las actuaciones de investigación.....	6
5.5.	Admisión, inadmisión y derivación a otros canales.	6
5.6.	Remisión al Ministerio Fiscal.	6
5.7.	Apertura de expediente de investigación interna.	7
5.8.	La investigación interna.....	7
5.9.	Conclusiones y propuesta de acciones.	7
5.10.	Seguimiento de las decisiones adoptadas.	7
VI.	RESOLUCIÓN DE CONSULTAS	7
VII.	CONSERVACIÓN DE LAS COMUNICACIONES	8
VIII.	CANALES EXTERNOS.....	8
IX.	ENTRADA EN VIGOR, DIFUSIÓN Y REVISIÓN.....	9



I. FINALIDAD Y OBJETO

El art.5.2.h) de la Ley 2/2023 de Protección al Informante establece como requisito de todo Sistema Interno de Información el *“contar con una política o estrategia que enuncie los principios generales en materia de Sistemas interno de información y defensa del informante y que sea debidamente publicitada en el seno de la entidad u organismo”*.

El Consejo de Administración de Radio Televisión Madrid, en adelante RTVM, como demostración de su compromiso en la toma de aquellas decisiones necesarias para la efectiva implantación de un Modelo de Organización y Gestión para la Prevención del Delito configura como uno de los pilares principales la implantación de un Sistema Interno de Información.

El objetivo de este Sistema es recibir y tramitar eficazmente comunicaciones relacionadas con los comportamientos que, en esencia, puedan suponer una vulneración del ordenamiento jurídico general, así como los principios contemplados en su Código Ético y de Conducta y otros documentos esenciales que conforman su Modelo de Prevención del Delito.

Para ello, la presente Política recoge las cuestiones relativas a la gestión y tramitación de las comunicaciones recibidas, con el objetivo de incorporar un modelo flexible y ágil conforme a la normativa legal vigente, estándares y mejores prácticas nacionales e internacionales, efectuando una distinción entre canales ordinarios y otros denominados alternativos en los que los potenciales informantes, podrán, sin miedo a represalia o a sufrir conductas perjudiciales, poner de manifiesto los hechos que supongan vulneraciones del Sistema de Compliance.

La presente Política, junto con el Procedimiento del Sistema Interno de Información que regula su funcionamiento, tienen como finalidad, garantizar una gestión profesional, confidencial, imparcial y de máxima protección durante todo el proceso, generando con ello un clima de confianza a los interesados.

II. ALCANCE

La presente Política resulta de aplicación a todas las actividades desarrolladas por la entidad y es de obligado cumplimiento por todos los miembros de esta, con independencia del cargo o puesto que ocupen dentro de la organización, la naturaleza jurídica de su relación y su ubicación geográfica.

III. PRINCIPIOS QUE RIGEN EL SISTEMA INTERNO DE INFORMACIÓN

Los principios generales que rigen el Sistema se deben respetar y garantizar por todos los miembros de la organización, con el fin de otorgar a los informantes una protección adecuada frente a las posibles represalias que puedan sufrir por el mero hecho de poner en conocimiento de la organización hechos que puedan suponer una vulneración del ordenamiento jurídico o de las normas internas.

El Sistema Interno de Información y el Canal habilitado como medio para recibir las comunicaciones se rigen por los siguientes principios:



3.1. Responsable del Sistema Interno de Información.

Se ha designado una persona física como responsable de la atención y gestión de las comunicaciones que lleguen en el marco del Sistema Interno de Información.

El Responsable del Sistema Interno de Información desarrollará 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.

La función de Responsable del Sistema Interno de Información ha sido asumida por la Función de Compliance, esto es, el Comité de Cumplimiento. El Comité delegará las facultades de gestión del Sistema interno de información y de tramitación de expedientes de investigación en alguno de sus miembros lo cual queda debidamente documentado en el correspondiente documento de nombramiento.

3.2. Accesibilidad

Todo el proceso de gestión de las comunicaciones que lleguen al Sistema Interno de Información y en especial su Canal interno serán claros, públicos y de fácil acceso a empleados y terceros que deseen realizar una comunicación, siendo el medio idóneo para que la entidad escuche y hable con todos sus miembros u otros terceros interesados.

3.3. Buena fe

El informante ha de actuar de buena fe y deberá basar la comunicación en hechos o indicios de los que razonablemente pueda desprenderse la realización de un comportamiento irregular, ilícito, delictivo o contrario a los principios y valores de la organización. Trasladar información a sabiendas de su falsedad de forma deliberada causando así un perjuicio podrá conllevar acciones disciplinarias.

3.4. Confidencialidad

Se garantizará en todo momento la protección de la confidencialidad en general. La identidad del informante tendrá la consideración de información confidencial y no podrá ser comunicada ni revelada sin su consentimiento.

3.5. Objetividad e imparcialidad

Una vez recibida una comunicación, se garantizará la imparcialidad, así como el derecho a la intimidad, a la defensa y a la presunción de inocencia de todas las personas objeto de la misma.

3.6. Transparencia

El Sistema Interno de Información y en especial su Canal interno se configuran como una herramienta de transparencia que favorece la confianza de las personas de la entidad.

3.7. Autoridad, independencia y conflicto de intereses

En todo momento, el Responsable del Sistema Interno de Información actuará con total autonomía e independencia. Si alguna de las personas participantes en la investigación está implicada en los hechos que se comuniquen o considera que puede incurrir en



algún tipo de conflicto de interés deberá abstenerse de participar en la gestión y posterior investigación.

3.8. Prohibición de represalias

Se garantiza que el hecho de comunicar una conducta que pueda suponer un incumplimiento o irregularidad no será objeto de ninguna represalia, directa o indirecta, contra aquellas personas que, de buena fe, hubieran realizado dicha comunicación.

3.9. Exención ante obligaciones contractuales.

No se restringirá la posibilidad de informar en base a obligaciones contractuales, tales como acuerdos de no divulgación, cláusulas relativas a confidencialidad comercial o laboral cuando el informante realice la comunicación en base a motivos razonables de pensar que ésta es necesaria para poner en conocimiento de la organización una acción u omisión de la normativa

IV. CONDUCTAS QUE SE PUEDEN COMUNICAR

La información sobre infracciones o incumplimientos se interpreta en un sentido amplio, esto es, se pueden comunicar hechos que puedan dar lugar a tener sospechas razonables, ser infracciones reales o potenciales, que se hayan producido o que sea probable que se produzcan.

A título ilustrativo, a continuación, se reseñan algunas de las posibles temáticas objeto de comunicación:

- Contratación pública. Corrupción, cohecho y tráfico de influencias.
- Transparencia y deberes contables.
- Prevención del blanqueo de capitales y financiación del terrorismo.
- Derechos de los trabajadores.
- Derechos y libertades fundamentales.
- Salud y bienestar de los animales.
- Protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información.
- Concesión de ayudas y subvenciones.
- Respeto e Igualdad.
- Acoso laboral y Acoso sexual.
- Medio ambiente.
- Obligaciones tributarias y seguridad social.
- Derechos de los consumidores y usuarios.



4.1. Garantías del informante

El Sistema Interno de Información en general y su Canal en particular disponen de las garantías necesarias para mantener la seguridad de las comunicaciones y confidencialidad entre el informante y el Comité de Cumplimiento.

El Responsable del Sistema Interno de Información tomará conocimiento del contenido de cada una de las comunicaciones y las tratará con la diligencia debida, guardando, siempre con la máxima confidencialidad, la identidad del informante cuando la comunicación no sea anónima.

Queda totalmente prohibida cualquier tipo de represalias sobre quienes informen de buena fe. Si se confirmara que dichas personas han sido objeto de cualquier tipo de represalia, estigmatización o vejación, los autores de ésta serán objeto de investigación y, en su caso, de sanción.

4.2. Garantías del posible implicado

Las personas presuntamente implicadas en los hechos sobre los que se informen nunca podrán ser sancionadas por una simple comunicación o notificación, siendo, en todo caso, necesario que se compruebe la veracidad de la comunicación y se les conceda la oportunidad de ofrecer una explicación a la situación comunicada.

Los posibles implicados serán informados por el Responsable del Sistema Interno de Información tan pronto como sea posible y, a más tardar, en el plazo de un (1) mes desde la recepción de la comunicación, de los hechos trasladados, el responsable de tramitar la comunicación, los siguientes hitos de la investigación y los derechos en protección de datos que le asisten.

Excepcionalmente, si existe riesgo importante de que la notificación al presunto implicado ponga en peligro la eficacia de la investigación o recopilación de pruebas, no se procederá a la notificación hasta que cese dicho riesgo.

Quedarán documentados y suficientemente razonados los motivos que inducen a concretar la existencia de dicho riesgo, pudiendo prorrogarse el plazo máximo de un mes previsto por un periodo no superior a tres meses.

La información relativa al posible implicado se tratará con estricta confidencialidad.

V. PRINCIPIOS ESENCIALES DEL PROCEDIMIENTO DE GESTIÓN DE LAS COMUNICACIONES

5.1. Principios rectores del procedimiento

Teniendo en cuenta las posibles consecuencias penales de los hechos que pueden ser comunicados a través del Sistema Interno de Información, 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.
- 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 entidad, evitando así que el informante haga un mal uso del Sistema Interno de Información.

- Contradicción: durante la investigación se habrá de permitir en todo momento al presunto implicado que pueda ejercer su derecho de defensa.

5.2. 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.

5.3. 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.

5.4. 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.

5.5. 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, siendo 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 concluida.

En este caso, se comunicará 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.

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

5.6. Remisión al Ministerio Fiscal.

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



5.7. Apertura de expediente de investigación interna.

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

El Responsable del Sistema Interno de Información, como miembro del Comité de Cumplimiento, será en principio el encargado de la investigación, salvo que se detecte una situación de conflicto de intereses, en cuyo caso se pondrá en conocimiento del resto de miembros del Comité que tomarán la decisión colegiada de nombrar un responsable alternativo, que podrá ser interno o externo.

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

En caso de que se consideren necesarias medidas urgentes de reacción o contención, el informe se trasladará a la Dirección General para que tenga conocimiento de esta información y, si procede, tome una decisión en relación con las medidas propuestas.

Igualmente, se pondrá a disposición del presunto implicado un resumen de los hechos y 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.

5.8. La investigación interna.

El Responsable del Sistema Interno de Información con apoyo del Comité de Cumplimiento, garantizará que la investigación disponga de todos los medios necesarios, ya sean internos o externos, 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 en función de las circunstancias concretas.

5.9. Conclusiones y propuesta de acciones.

Una vez finalizada la investigación en los plazos establecidos se elaborará un informe de conclusiones y propuesta de actuación.

5.10. Seguimiento de las decisiones adoptadas.

Tras la finalización de la investigación y una vez efectuada la toma de decisiones, El Responsable del Sistema Interno de Información con apoyo del Comité de Cumplimiento hará el 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 la gestión del Sistema Interno de Información a la mejora continua del Modelo de Prevención del Delito de la entidad y a reforzar la cultura de Compliance.

VI. RESOLUCIÓN DE CONSULTAS

El canal podrá ser igualmente utilizado como fuente interna de recepción de consultas y dudas sobre el propio proceso de comunicación de irregularidades o sobre la



aplicación de las políticas internas o al cumplimiento de las obligaciones legales que afecten a la entidad.

VII. CONSERVACIÓN DE LAS COMUNICACIONES

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 en 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.

Los datos personales serán conservados en el entorno del canal por un periodo máximo de tres meses desde la comunicación. Transcurrido este tiempo, si los datos fueran necesarios para continuar la investigación de los hechos, podrán seguir siendo tratados a los efectos de la investigación realizada o, en su caso, desde la finalización del procedimiento disciplinario, administrativo o judicial al que hubieran dado inicio.

Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada.

Concluida la investigación, se podrá conservar por el responsable designado al efecto la información imprescindible para garantizar la trazabilidad, el cumplimiento y la eficacia del Sistema Interno de Información y del Modelo de Prevención del Delito en el que queda integrado.

VIII. CANALES EXTERNOS.

Se informa de la existencia de canales externos de información ante autoridades competentes.

Actualmente, se informa de la existencia de los siguientes canales externos que podrían ser de interés en función del sector de actividad de la organización y su ámbito de actuación territorial:

- ✓ 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)
- ✓ Oficina Andaluza contra el Fraude y la Corrupción
- ✓ Oficina Antifraude de Cataluña (OAC)
- ✓ Buzón Ético y de Buen Gobierno del Ayuntamiento de Barcelona;
- ✓ Oficina Municipal contra el Fraude y la Corrupción del Ayuntamiento de Madrid.
- ✓ Oficina de Prevención y Lucha contra la Corrupción en las Illes Balears



IX. ENTRADA EN VIGOR, DIFUSIÓN Y REVISIÓN

La entrada en vigor de la presente Política tendrá lugar en el mismo momento de la fecha de aprobación, modificación o actualización del presente documento.

Será objeto de publicación y difusión para su adecuado conocimiento, encontrándose a disposición y consulta a través de la sede electrónica de la sociedad publicada en <https://transparencia.telemadrid.es/>; de la sección corporativa de su página su página web www.telemadrid.es y en la intranet corporativa.

Con carácter ordinario, se revisará el contenido con la periodicidad establecida en su sistema de información documentada y de forma extraordinaria cuando concurren circunstancias significativas de carácter legal, organizativo o de cualquier otra naturaleza que justifique su adaptación y/o actualización inmediata.

Aprobado por el Consejo de Administración de RTVM, el 11 de diciembre de 2023.