

# **POLÍTICA DEL SISTEMA INTERNO DE INFORMACIÓN**

**CONTROL DE CAMBIOS**

<b>Fecha</b>	<b>Cambios Realizados</b>	<b>Versión</b>	<b>Fecha de aprobación</b>
Diciembre 2023	Primera Redacción	1.0	29/12/2023
Septiembre 2024	Inclusión de los canales externos (punto 7).	2.0	27/09/2024
Diciembre 2024	Creación de la A.I.P.I. (punto 7).	3.0	27/12/2024
Junio 2025	Acceso al RCTIR (punto 8).	4.0	27/06/2025
Marzo 2026	Habilitación del canal externo de la AIPI (punto 7)	5.0	20/03/2026

## Contenido

1. Introducción .....	4
2. Objetivo.....	4
3. Alcance .....	4
3.1. Ámbito material de aplicación .....	4
3.2. Ámbito personal de aplicación .....	5
4. Principios generales de actuación .....	5
5. Responsable del Sistema interno de información y personal con acceso a la información .....	6
6. Canales internos de recepción de informaciones .....	7
7. Canales externos .....	7
8. Acceso al RCTIR.....	8
9. Aprobación y modificaciones .....	9

## 1. Introducción

La colaboración ciudadana es un elemento clave en el Estado de Derecho español, ya que no solo se manifiesta en el correcto cumplimiento de las obligaciones personales, sino también en el compromiso colectivo con el buen funcionamiento de las instituciones públicas y privadas. La colaboración ciudadana también se contempla como un deber de todo ciudadano cuando presencia la comisión de un delito.

Además, en algunos ámbitos, como el financiero o de defensa de la competencia, se han incorporado instrumentos específicos para que los ciudadanos puedan facilitar a los organismos supervisores información útil sobre actuaciones irregulares o ilegales. También existen casos en los que las actuaciones cívicas han permitido impulsar investigaciones que han concluido con la imposición de la correspondiente condena penal por comportamientos irregulares o corruptos.

Es importante destacar que el ordenamiento jurídico debe proteger a los ciudadanos que informan sobre vulneraciones del ordenamiento jurídico en el marco de una relación profesional ya que, en ocasiones, estos comportamientos cívicos han generado consecuencias penosas para quienes han comunicado tales prácticas corruptas y otras infracciones. Por lo tanto, resulta indispensable asentar en la sociedad la conciencia de que debe perseguirse a quienes quebrantan la ley y que no deben consentirse ni silenciarse los incumplimientos.

## 2. Objetivo

El objetivo de esta política es enunciar los principios generales de actuación que rigen en el **Sistema interno de información** y defensa del informante (en adelante, Sistema) definido en Key Capital Partners, Agencia de Valores, S.A. (en adelante, la Entidad) y publicitarla con la finalidad de colaborar en el compromiso colectivo con el buen funcionamiento de las instituciones públicas y privadas.

La Entidad garantiza una protección adecuada a aquellos informantes ante las posibles represalias que pudieran sufrir y fortalece la cultura de la información y la infraestructura de integridad de la entidad y fomenta la cultura de la información como mecanismo para prevenir y detectar amenazas al interés público mediante la implantación de este Sistema.

## 3. Alcance

### 3.1. Ámbito material de aplicación

El Sistema es de aplicación para cualquier comunicación realizada por un informante que suponga una acción u omisión que pueda ser constitutiva de **infracción penal o administrativa grave o muy grave** o que pueda constituir una infracción 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 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019;
2. Afecten a los intereses financieros de la Unión Europea; o
3. Incidan en el mercado interior.

Dicho lo anterior, en el caso de que se comunicara una información fuera de este ámbito material de aplicación la Entidad se reserva el uso de darle curso a su investigación, pero el informante no estaría cubierto por las medidas de protección ante represalias.

### 3.2. Ámbito personal de aplicación

El Sistema es de aplicación a los informantes que hayan obtenido información sobre una infracción en un **contexto laboral o profesional**, comprendiendo en todo caso:

- a) las personas que tengan la condición de trabajadores por cuenta ajena;
- b) los autónomos;
- c) los accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de la Entidad, incluidos los miembros no ejecutivos;
- d) cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores;

También será de aplicación a los informantes que comuniquen información sobre una infracción obtenida en el marco de una relación laboral o estatutaria ya finalizada, becarios, trabajadores en 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 obtenida durante el proceso de selección o de negociación precontractual.

Las medidas de protección del informante 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 y a cualquier persona física o jurídica en la que preste servicios el informante o le asistan al mismo o que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante.

### 4. Principios generales de actuación

La Entidad ha implantado un Sistema interno de información basado en los siguientes principios generales de actuación:

1. Actuar, en todo momento, al amparo de la **legislación vigente** y dentro del marco establecido por el Reglamento Interno de Conducta, y dando cumplimiento a la normativa interna de la Entidad. En particular, se dará cumplimiento a todos los requisitos recogidos 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.
2. **Integrar** y coordinar los distintos **canales** internos de información que pudieran establecerse dentro de la entidad.
3. Contar con un procedimiento de **gestión** de informaciones recibidas.
4. Generar un entorno de **transparencia** y **accesibilidad** tanto a los canales internos como a los externos para favorecer la comunicación de posibles infracciones por parte de aquellas personas incluidas en el ámbito personal de aplicación. Se permitirá incluso la presentación y posterior tramitación de comunicaciones anónimas.
5. Ser **independiente** y **autónomo**, apareciendo diferenciado respecto de los sistemas internos de información de otras entidades.
6. Garantizar la **confidencialidad** de la información comunicada incluso por cauces no habituales y de las actuaciones que se desarrollen en su gestión y tramitación, así como el secreto de las comunicaciones.

7. Cumplir con los requisitos establecidos en normativa en materia de **protección de datos de carácter personal**.
8. Implementar programas adecuados de **formación** específicos a las personas involucradas en el acceso a los datos objeto de comunicación y genéricos para el resto de la organización.
9. **Investigar y sancionar los actos y conductas irregulares** de manera justa, no discriminatoria y proporcional a lo dispuesto en el régimen disciplinario. Dentro de las mismas se encontrarían las denuncias falsas o de mala fe.
10. Promover un **ambiente y cultura** que garantice la efectividad y la idoneidad de su funcionamiento para poder conocer en primer lugar una posible irregularidad y no dejar espacios de impunidad contra el informante.
11. Designar un **responsable del Sistema** evitando posibles situaciones de conflicto de interés asignándole los recursos financieros, humanos y técnicos necesarios.
12. Establecer **garantías** para la protección de los informantes, prohibiendo las represalias al denunciante y pleno acceso a las medidas de apoyo.
13. Garantizar el **derecho de las personas afectadas** a que sean informadas y a ser oída en cualquier momento.
14. Respetar la **presunción de inocencia** y el honor de las personas afectadas.
15. Remitir la información al **Ministerio Fiscal** con carácter inmediato 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.

##### **5. Responsable del Sistema interno de información y personal con acceso a la información**

El Consejo de Administración, como máximo responsable de la implantación del Sistema interno de información, ha nombrado Responsable del Sistema a la Responsable de la Unidad de Cumplimiento Normativo y Gestión de Riesgos, Doña María Victoria Madero Jiménez, quien ejercerá su cargo con independencia.

El Responsable del Sistema responderá de la tramitación diligente de las informaciones recibidas a través de los canales internos.

El acceso a los datos personales contenidos en el Sistema interno de información quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente a:

- a) El Responsable del Sistema.
- b) El responsable de recursos humanos, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.
- c) El responsable de los servicios jurídicos de la entidad.
- d) Los encargados del tratamiento que eventualmente se designen.
- e) El delegado de protección de datos.

Dicho lo anterior, será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas

correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

## **6. Canales internos de recepción de informaciones**

La Entidad cuenta con dos canales internos para la recepción de informaciones, uno principal, consistente en un buzón electrónico el cual se encuentra accesible a través de la dirección pública:

[https://keycapital.com/wp-content/uploads/2025/07/Politica-del-Sistema-Interno-de-  
Informacion Key-Capital-Partners v4.pdf](https://keycapital.com/wp-content/uploads/2025/07/Politica-del-Sistema-Interno-de-Informacion-Key-Capital-Partners_v4.pdf)

y otro alternativo, a solicitud del informante, consistente en la posibilidad de requerir una reunión presencial al Responsable del Sistema.

Todo el personal no responsable del tratamiento del canal interno queda advertido que deberán guardar la debida confidencialidad en caso de que cualquier comunicación no sea remitida por el canal interno principal fijado (buzón electrónico) constituyendo una infracción muy grave su quebranto y que deberán transmitirla inmediatamente al Responsable del Sistema.

## **7. Canales externos**

Además de utilizar el canal interno de la Entidad que se desarrolla en este documento, toda persona física que lo desee puede presentar su información a través del canal externo de información de la Autoridad Independiente de Protección del Informante (A.I.P.I.), al que la Ley dedica el Título III.

El acceso a dicho canal externo se encuentra disponible a través de la página web oficial de la Autoridad Independiente de Protección del Informante: <https://www.proteccioninformante.gob.es/>

Dicho canal permite la presentación de comunicaciones tanto de forma identificada como anónima, en los términos previstos en la normativa aplicable.

El Real Decreto 1101/2024, de 29 de octubre, aprueba el Estatuto de la Autoridad Independiente de Protección del Informante, (A.A.I.), y en él se establece que los nombramientos y ceses, tanto de las personas físicas como de las personas integrantes del órgano colegiado que hayan sido designadas como Responsables del Sistema interno de información desde la entrada en vigor de conformidad con lo previsto en el artículo 8.3 de la Ley 2/2023.

En este sentido, una vez habilitado el canal correspondiente por parte de la Autoridad Independiente de Protección del Informante, la Sociedad ha procedido a dar cumplimiento a dicha obligación de comunicación del Responsable del Sistema Interno de Información (RSII), habiéndose realizado las siguientes comunicaciones:

- Con fecha 05.02.2026, comunicación al Consejo de Transparencia y Protección de Datos.
- Con fecha 10.02.2026, comunicación al Registro General de la Autoridad Independiente de Protección del Informante.

Al margen de lo expuesto, cualquier persona que tenga conocimiento de hechos que pudieran ser constitutivos de fraude o irregularidad en relación con proyectos u operaciones financiados total o parcialmente con cargo a fondos procedentes de la Unión Europea podrá poner dichos hechos en conocimiento del Servicio Nacional de Coordinación Antifraude S.N.C.A. a través del canal habilitado al efecto por dicho Servicio (Infofraude) en la dirección web:

<https://www.igae.pap.hacienda.gob.es/sitios/igae/esES/snca/Paginas/ComunicacionSNCA.aspx>

O bien acudir a la Oficina Europea de Lucha contra el Fraude (OLAF), la información al respecto se desarrolla en el siguiente enlace:

[https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud\\_es](https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_es)

O, finalmente, a la Fiscalía Europea, sobre la que se dispone de la información al respecto en el siguiente enlace:

<https://www.eppo.europa.eu/en/reporting-crime-eppo>

En el caso de que se trate de una información sobre posibles prácticas anticompetitivas, podrán utilizarse los canales externos de comunicaciones de la Dirección de Competencia de la Comisión Nacional de los Mercados y la Competencia, cuya información al respecto se desarrolla en el siguiente enlace:

<https://edi.cnmc.es/buzones-anonimos/sica>

Lo anterior se entiende sin perjuicio del derecho de cualquier informante a acudir a otras autoridades administrativas, judiciales o europeas competentes, de conformidad con lo previsto en la normativa aplicable.

## **8. Acceso al RCTIR.**

La Entidad, en su calidad de sujeto obligado en virtud de lo dispuesto en el artículo 2 de la Ley 10/2010, de 28 de abril presentó el día 3 de julio de 2025 ante el Registro Central de Titularidades Reales (RCTIR) una solicitud inicial en que acreditó su condición de sujeto obligado, que fue aceptada procediendo acto seguido la Entidad a designar las personas físicas que accederán al RCTIR en su nombre.

De acuerdo con el artículo 5.2 del reglamento del RCTIR (Real Decreto 609/2023, de 11 de julio, por el que se crea el Registro Central de Titularidades Reales y se aprueba su Reglamento), la Entidad, al igual que el resto de los sujetos obligados de la Ley 10/2010, de 28 de abril, tendrán acceso a la información vigente contenida en el Registro Central y podrán recabar certificación electrónica del RCTIR o un extracto de este para el cumplimiento de sus obligaciones en materia de identificación del titular real. Así mismo, podrán obtener información sobre la naturaleza y alcance del interés real ostentado y de esta titularidad real, en particular, al dato de si la misma se debe al control de la propiedad o al del órgano de gestión de la misma y el porcentaje de participación, con inclusión, en el caso de propiedad indirecta, de la información sobre las personas jurídicas interpuestas y su participación en cada una de ellas.

Se presumirá acreditado el interés legítimo de la Entidad así como resto de sujetos obligados a que se refiere el artículo 2 de la Ley 10/2010, de 28 de abril, para acceder a la información y recabar certificación al efecto del Registro Central, dado que se realiza para cumplir con sus obligaciones de diligencia debida, siempre que expresen la causa

de la consulta, ya sea para un supuesto específico o con carácter general, y ésta sea acorde con la finalidad del Registro.

## **9. Aprobación y modificaciones**

El contenido de esta Política se somete a aprobación por el Consejo de Administración. Cualquier modificación de su contenido como consecuencia de la mejora continua del sistema debe ser aprobada por el mismo.