

## POLÍTICA DEL SISTEMA INTERNO DE INFORMACIÓN

### 1. CONTROL DE CAMBIOS

| Versión | Fecha      | Descripción de cambios                                                                                                                                                                                                                           | Aprobación         |
|---------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| 1       | 22/04/2026 | Implantación del Sistema Interno de Información de conformidad con las disposiciones de 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. | Órgano de Gobierno |

### 2. ÍNDICE

|       |                                                                         |    |
|-------|-------------------------------------------------------------------------|----|
| I.    | INTRODUCCIÓN .....                                                      | 1  |
| II.   | OBJETO .....                                                            | 2  |
| IV.   | ÁMBITO DE APLICACIÓN .....                                              | 2  |
| V.    | SISTEMA INTERNO DE INFORMACIÓN .....                                    | 3  |
| VI.   | CANAL EXTERNO DE INFORMACIÓN .....                                      | 5  |
| VII.  | RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN.....                     | 5  |
| VIII. | CONTENIDO DE LAS COMUNICACIONES QUE SE REALICEN A TRAVÉS DEL CANAL..... | 6  |
| IX.   | PROTECCIÓN DE DATOS PERSONALES. CLÁUSULA DE PROTECCIÓN DE DATOS .....   | 7  |
| X.    | PROCEDIMIENTO DE INVESTIGACIÓN.....                                     | 9  |
| XI.   | VIGENCIA Y ACTUALIZACIÓN.....                                           | 10 |

### 3. CONTENIDO

#### I. INTRODUCCIÓN

En cumplimiento de 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 (en adelante, «la Ley 2/2023»), KENSINGTON SCHOOL, C.B (en adelante EL COLEGIO) ha implantado un Sistema Interno de Información (en adelante, SII) como instrumento esencial para promover la integridad, la transparencia y el cumplimiento normativo en la organización.

El SII se configura como el cauce preferente para canalizar, de forma segura, confidencial y eficiente, las denuncias o comunicaciones sobre acciones u omisiones que puedan constituir infracciones graves o muy graves en el marco de la Ley. El sistema garantiza la protección de las personas informantes, de quienes les asistan y de aquellas que estén vinculadas a ellas, asegurando el adecuado tratamiento de sus datos personales y la confidencialidad de sus identidades, salvo en los supuestos de comunicación a autoridades competentes previstos legalmente.

La organización y gestión del SII se articula a través de un canal interno de información como vía preferente de comunicación, integrando los demás cauces que puedan habilitarse conforme a

la normativa aplicable y preservando en todo momento la seguridad de la información y la protección de datos personales. Asimismo, se adoptan medidas específicas para suprimir los datos que no resulten pertinentes para la investigación y se prohíbe el tratamiento de información innecesaria.

El SII constituye un sistema único e independiente, que integra los diferentes canales internos de información conforme a lo establecido en la Ley 2/2023; las comunicaciones que se reciban por otros medios y se encuentren comprendidas en su ámbito de aplicación serán redirigidas a dicho sistema.

Mediante el SII, EL COLEGIO reafirma su compromiso con la prevención, detección y gestión eficaz de actuaciones irregulares, promoviendo una cultura organizativa basada en la ética, la legalidad y la ausencia de represalias frente a las personas informantes.

Todas las actuaciones desarrolladas en el marco del SII se ajustarán a los principios y garantías establecidos en la Ley 2/2023 y en sus normas de desarrollo.

## **II. OBJETO**

El objeto de la presente Política es establecer los principios y procedimientos para la implantación y funcionamiento del Sistema Interno de Información de EL COLEGIO, en cumplimiento de lo dispuesto en la Ley 2/2023.

Esta Política establece el marco para una cultura de información responsable, fomentando la comunicación interna y la adecuada canalización de las denuncias o alertas recibidas, con pleno respeto a las garantías legales de confidencialidad, ausencia de represalias y protección integral de los derechos de los informantes y de las personas afectadas, en el marco de lo dispuesto por la Ley 2/2023.

## **III. ALCANCE**

La presente Política resulta de aplicación a EL COLEGIO y que, de acuerdo con lo dispuesto en el ámbito de aplicación de la Ley 2/2023, de 20 de febrero, se encuentra obligada a disponer de un Sistema Interno de Información, así como a las personas trabajadoras que, conforme a dicha normativa, puedan presentar comunicaciones a través del Sistema Interno de Información en un contexto laboral o profesional.

## **IV. ÁMBITO DE APLICACIÓN**

De acuerdo con la Ley 2/2023, de 20 de febrero, el ámbito de aplicación de esta política se extiende a cualquier informante que necesite poner en conocimiento EL COLEGIO posibles incumplimientos incluidos en dicha norma, siempre que estén relacionados con las siguientes personas:

- a. Trabajadores por cuenta ajena.
- b. Autónomos.
- c. Accionistas, partícipes y miembros del órgano de administración, dirección o supervisión, incluidos los miembros no ejecutivos.
- d. Trabajadores bajo supervisión y dirección de contratistas, subcontratistas o proveedores.

- e. Extrabajadores, voluntarios, becarios, candidatos, trabajadores en periodos de formación o personas en relación precontractual.
- f. Representantes de los trabajadores, cuando actúen en funciones de asesoramiento y apoyo al informante.
- g. Personas relacionadas con el informante, que le presten servicios o asistan al mismo.

## **V. EL SISTEMA INTERNO DE INFORMACIÓN DE EL COLEGIO**

### **a. Implantación.**

La implantación del Sistema Interno de Información de EL COLEGIO y de la presente Política corresponde al Órgano de Gobierno, que delega su ejecución y supervisión en el responsable designado del SII.

El responsable del SII, como figura encargada de la puesta en marcha, desarrollo y correcto funcionamiento del canal de comunicación, podrá, para el adecuado desempeño de sus funciones y responsabilidades, requerir la intervención, asistencia o asesoramiento de asesores y consultores externos con la finalidad de garantizar el cumplimiento de todos los requisitos legales y de las mejores prácticas en la materia.

La presente Política y el Sistema Interno de Información serán revisados y, en su caso, actualizados periódicamente, atendiendo a las modificaciones legales, recomendaciones de organismos reguladores, o resultados de evaluaciones internas, manteniendo el compromiso con la mejora continua.

Asimismo, se garantiza la participación del área de Recursos Humanos para la realización de la consulta previa a la representación de las personas trabajadoras, en los términos previstos en la Ley 2/2023.

### **b. Reglas de funcionamiento.**

El SII es el cauce que EL COLEGIO pone a disposición de los informantes para que, en un contexto laboral o profesional puedan comunicar hechos de los que sean testigos o tengan conocimiento y que puedan constituir: (i) infracciones del Derecho de la Unión Europea; (ii) infracciones penales o infracciones administrativas de carácter grave o muy grave.

Las comunicaciones deberán referirse a hechos o conductas realizadas por personas integrantes del Órgano de Gobierno, Alta Dirección, directores, responsables, personal, socios comerciales, o cualesquiera partes interesadas de EL COLEGIO. Quedan comprendidas en el SII las infracciones en materia de seguridad y salud en el trabajo.

Asimismo, se integran en el SII las comunicaciones relativas a posibles infracciones de la normativa de protección de datos quedando excluidas las consultas, dudas o el ejercicio de derechos, que se gestionarán a través del canal habitual de protección de datos.

El SII podrá recibir otras comunicaciones fuera del ámbito de aplicación, pero dichas comunicaciones y sus remitentes quedarán fuera del ámbito de protección de la Ley 2/2023.

### **c. Principios del SII**

Los principios que rigen el Sistema Interno de Información de EL COLEGIO son los siguientes:

- **Accesibilidad:** El Sistema Interno de Información de EL COLEGIO garantiza un acceso sencillo y directo a todas las personas comprendidas en su ámbito de aplicación, con independencia de su posición, conocimientos técnicos, ubicación, idioma o capacidades. Las comunicaciones podrán presentarse por escrito u oralmente, de forma identificada o anónima, y el informante podrá solicitar la celebración de una reunión presencial para formalizar la comunicación que se celebrará dentro del plazo máximo de siete (7) días desde la solicitud. Además, se advertirá al informante de que la comunicación será grabada en su caso y se le informará del tratamiento de sus datos de acuerdo con el RGPD antes de proceder a la grabación/transcripción.
- **Confidencialidad y Protección de datos:** Se garantiza en todo momento la confidencialidad de la identidad del informante y de terceros mencionados en la comunicación, así como la protección de datos personales tratados, limitando el acceso a la información al personal autorizado a los hechos y datos personales. No obstante, los datos podrán comunicarse a las autoridades administrativas o judiciales cuando así se requiera en el marco de un procedimiento o cuando los hechos pudieran ser indiciariamente constitutivos de delito. El SII adoptará las medidas técnicas y organizativas adecuadas para que no se obtengan datos que permitan la identificación del informante salvo los supuestos previstos legalmente.
- **Efectividad y Garantía de tratamiento:** El SII asegura que todas las comunicaciones sean gestionadas de manera ágil, exhaustiva y eficaz, permitiendo a la organización detectar, prevenir y corregir con prontitud posibles irregularidades. Se garantizará en todo momento el cumplimiento de los requisitos legales y procedimentales establecidos.
- **Presunción de Inocencia:** Se garantiza la presunción de inocencia, el derecho de defensa y la salvaguarda del derecho al honor de las personas afectadas por la comunicación. Estas personas tendrán derecho a conocer los hechos u omisiones que se les atribuyen, y a ser oídas en el marco de la investigación.
- **Protección y No Represalia:** Se prohíbe expresamente cualquier forma de represalia contra las personas que formulen comunicaciones de buena fe, así como contra quienes les asistan o estén vinculados a ellas. Esta protección se extiende, en los términos de la Ley 2/2023, a familiares, personas trabajadoras y a las personas jurídicas con las que el informante mantenga una relación laboral o profesional. EL COLEGIO recoge esta garantía de no represalia en su Código Ético y dispone de los medios y garantías necesarios para hacerla efectiva.
- **Objetividad e Imparcialidad:** Toda la información recibida será analizada y valorada de forma objetiva sin que la identidad de la persona informante o de las personas afectadas determine un trato diferente y privilegiado.
- **Transparencia:** El SII es una herramienta de transparencia que refuerza la confianza de las partes interesadas. Se proporcionará información a la persona informante, y, cuando proceda a las personas afectadas sobre la tramitación y el estado de la comunicación, y se dará publicidad adecuada a esta Política, a los canales habilitados y a la información que se considere necesaria a efectos de transparencia.

## VI. CANAL EXTERNO DE INFORMACIÓN

Sin perjuicio de que el Sistema Interno de información de EL COLEGIO es el cauce preferente para reporte de las informaciones descritas en esta Política, los informantes podrán acudir a los canales externos de información habilitados por autoridades competentes, como: la Autoridad Independiente de Protección del Informante (AIPI), la autoridad competente de su comunidad autónoma, instituciones, órganos u organismos de la Unión Europea, según sea el caso. Asimismo, a quienes realicen la comunicación a través del SII se les informará, de forma clara y accesible, sobre los canales externos de información.

## VII. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN.

El encargado de gestionar, tramitar y dar respuesta a las comunicaciones que se presenten a través del Sistema Interno de Información será el responsable del Sistema Interno de Información de la sociedad receptora de la comunicación, actuando con independencia y autonomía respecto del resto de órganos de dicha sociedad y disponiendo de los medios personales y materiales necesarios para el desempeño de sus funciones.

Se designará una persona sustituta del responsable del SII, para que asuma sus funciones cuando concurran circunstancias que impidan a este el ejercicio de estas.

Una vez recibida una comunicación en el SII, deberá emitirse acuse de recibo en un plazo no superior a **siete (7) días**, salvo que ello pueda comprometer la confidencialidad de esta. Las actuaciones de investigación no podrán, con carácter general, exceder el plazo de tres (3) meses desde la recepción de la comunicación, plazo que podrá ampliarse por otros tres (3) meses adicionales en supuestos de especial complejidad. El Departamento de Recursos Humanos podrá colaborar en aquellos expedientes en los que resulte necesario.

Todas las personas que intervengan en la gestión o tramitación del Sistema Interno de Información habrán de suscribir un compromiso de confidencialidad sobre el contenido de las comunicaciones y de la información a la que tengan acceso.

En el acuse de recibo remitido al autor de la comunicación se le informará debidamente sobre el tratamiento de sus datos personales y se le facilitará la correspondiente cláusula informativa, de conformidad con los artículos 12, 13 y 14 del RGPD y el artículo 11 de la LOPDGDD.

El responsable del Sistema Interno de Información es el único destinatario inicial y gestor de las comunicaciones recibidas a través del SII. Asimismo, llevará un libro-registro de las comunicaciones recibidas y de la tramitación dada a cada una de ellas que tendrá en todo caso carácter **CONFIDENCIAL**. 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.

La externalización de la gestión del Sistema Interno de Información podrá llevarse a cabo cuando así lo determine el responsable del Sistema Interno de Información y siempre que el tercero externo seleccionado ofrezca garantías efectivas de independencia, confidencialidad y secreto profesional en la prestación de este servicio. El cumplimiento de los requisitos de idoneidad, independencia y protección de datos será objeto de verificación previa y durante toda la relación contractual.

Los datos personales contenidos en el libro-registro de informaciones y de las investigaciones internas solo se conservarán durante el período necesario y proporcionado para cumplir con la Ley 2/2023 y, en ningún caso, por un período superior a diez años. Los datos personales del contenido de las comunicaciones se conservarán únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación y, en todo caso, se suprimirán transcurridos tres (3) meses desde la recepción de la comunicación si no se hubieran iniciado actuaciones, salvo conservación anonimizada exclusivamente como evidencia del correcto funcionamiento del sistema.

## VIII. CONTENIDO DE LAS COMUNICACIONES QUE SE REALICEN A TRAVÉS DEL CANAL

### a. Identificación.

Se admiten comunicaciones anónimas que serán examinadas y valoradas en función de su veracidad y suficiencia conforme al ámbito de aplicación de la Ley 2/2023.

Al hacer la comunicación, el informante podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones.

Si tras el análisis inicial se aprecia que la comunicación no encaja en el ámbito de aplicación de la Ley 2/2023, el responsable del SII procederá a su archivo y a la supresión de los datos personales contenidos en la misma.

Aunque se admiten comunicaciones anónimas, se recomienda la identificación del informante mediante nombre y apellidos, número de teléfono y dirección de correo electrónico.

### b. Forma.

Existe un único Sistema Interno de Información (SII), independiente y exclusivo conforme a la Ley 2/2023, siendo el resto de los canales habilitados exclusivamente para cuestiones, reclamaciones o consultas concretas ajenas al ámbito propiamente protegido por dicha norma.

El Sistema Interno de Información permite presentar las comunicaciones de las siguientes formas:

**Comunicaciones verbales:** por mensaje de voz o reuniones presenciales a solicitud del informante a Cristina Cobos García.

Previo consentimiento del informante, se podrán realizar mediante transcripción completa y exacta de la conversación elaborada por el responsable del SII o mediante una grabación en formato seguro, duradero y accesible. En su caso, se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo con lo que establece el RGPD. El informante podrá comprobar, rectificar y firmar la transcripción.

**Comunicaciones por escrito:** remitidas por correo postal a [compliancemanager@kensingtonschoolbcn.com](mailto:compliancemanager@kensingtonschoolbcn.com)

Solo en caso de materias claramente ajenas al ámbito de la Ley 2/2023 (p. ej., ejercicio de derechos en materia de protección de datos, cuestiones laborales o consultas generales), podrán ser empleados canales específicos y, si la información encajase en el SII, será redirigida a dicho sistema único de información.

Para estas comunicaciones se encuentran habilitados los siguientes canales:

**Canal Protección de Datos:** Para el ejercicio de derechos, y consultas relativas a la normativa de protección de datos. Responsable: Delegado de Protección de Datos; correo electrónico: [dpo@kensingtonschoolbcn.com](mailto:dpo@kensingtonschoolbcn.com)

**Canal de Recursos Humanos:** Para cuestiones laborales. Responsable: Dpto. de RRHH, correo: [ccobos@kensingtonschoolbcn.com](mailto:ccobos@kensingtonschoolbcn.com)

**Canal Dirección Postal:** Para cualquier tipo de información, remitida a Carrer dels Cavallers 31/33, 08034, Barcelona.

Las comunicaciones deberán describir la causa por la que el informante tiene conocimiento de los hechos y seguir, en la medida de lo posible el esquema de las siguientes preguntas: **¿Cuándo? ¿Dónde? ¿Quién? y ¿Qué?**

Las comunicaciones deben ser precisas, completas, objetivas, asépticas y respetuosas, evitando juicios de valor, omisiones o expresiones ofensivas. La ambigüedad en la descripción de los hechos no impedirá las indagaciones pertinentes.

EL COLEGIO pone a disposición de los informantes el **Modelo de Comunicación (Anexo I)**; utilizándose, en su defecto, el esquema indicado.

Las comunicaciones deberán realizarse de buena fe, y versar sobre hechos y personas que el informante considere veraces. Las comunicaciones formuladas de mala fe o con conocimiento de su falsedad, serán inadmitidas, y se procederá a la supresión de los datos personales que contengan, sin perjuicio de las responsabilidades que pudieran corresponder. Si se acreditara que la información facilitada o parte de ella no es veraz, se procederá a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, excepto si tal falta de veracidad pudiera constituir un ilícito penal, en cuyo caso se conservará la información por el tiempo necesario mientras se tramite el procedimiento judicial.

En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones previstas en la Ley 2/2023, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán los datos personales que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la Ley 2/2023.

## **IX. PROTECCIÓN DE DATOS PERSONALES. CLÁUSULA DE PROTECCIÓN DE DATOS**

KENSINGTON SCHOOL, C.B., garantiza la privacidad y confidencialidad de la información tratada a través del Sistema Interno de Información, y aplica medidas técnicas y organizativas apropiadas para proteger los datos personales frente a destrucción, pérdida, alteración, comunicación o acceso no autorizado. El acceso a la información se limita estrictamente a las personas autorizadas y se mantienen registros de acceso y actuaciones de acuerdo con los principios de minimización, necesidad y confidencialidad.

**1. Responsable de Tratamiento.**

KENSINGTON SCHOOL, C.B.

**2. Finalidad.**

Gestionar, tramitar y, investigar las comunicaciones recibidas a través del SII, incluyendo la adopción de medidas internas y el seguimiento de actuaciones derivadas, en el marco de la Ley 2/2023, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. La información recibida se utilizará exclusivamente para las finalidades previstas en el marco del SII y con las garantías de confidencialidad establecidas.

**3. Base jurídica (art. 6 RGPD).**

El tratamiento es necesario para el cumplimiento de una obligación legal conforme a la Ley 2/2023 (art. 6.1.c RGPD).

**4. Denuncias anónimas**

El SII permite la presentación de comunicaciones anónimas. El informante puede no facilitar datos identificativos.

No obstante:

- El contenido de la comunicación puede incluir datos personales de terceros (p. ej., de la persona afectada, testigos, etc.).
- Por razones de seguridad y funcionamiento del sistema, el proveedor tecnológico podría generar registros técnicos (p. ej., logs de seguridad, prevención de fraude o ciberataques). EL COLEGIO procurará que dichos registros se minimicen y se limiten a lo estrictamente necesario, con acceso restringido y medidas de seguridad adecuadas.
- Para preservar la confidencialidad, se aconseja el uso de dispositivos, redes seguras y, si se desea, navegación privada.

**5. Categorías de interesados y datos tratados**

Las categorías de datos personales tratados variarán en función de su participación:

- Informante: (si se identifica) datos identificativos y de contacto, datos profesionales / relación con la organización y el contenido de la comunicación.
- Persona Afectada por la información comunicada: datos identificativos y profesionales y, cualesquiera otros datos estrictamente necesarios para analizar y tramitar los hechos comunicados.
- Testigos / terceros: datos identificativos y de contacto y en su caso datos profesionales.

Los datos se obtienen de la información aportada a través del SII y, en su caso de la información recabada durante las actuaciones internas estrictamente necesarias.

**6. Datos de categorías especiales (art. 9 RGPD)**

Se solicita al informante que no incluya datos de categorías especiales (p. ej., salud, ideología, religión, afiliación sindical, orientación sexual, biométricos, etc.) salvo que sea imprescindible.

Si la comunicación incluyera datos de categorías especiales, estos serán suprimidos de forma inmediata en el SII, conforme a la Ley 2/2023. Cuando la naturaleza de los hechos exija su tratamiento para la adecuada tramitación, la gestión se articulará a través del procedimiento competente con las garantías y base jurídica aplicables, limitándose en el SII al contenido mínimo imprescindible.

## **7. Destinatarios / personas autorizadas**

El acceso directo se restringe a quienes, por sus funciones, deban conocer la información para la correcta tramitación, y solo durante el tiempo imprescindible:

- Responsable del SII, y personal expresamente autorizado para su gestión.
- Delegado de Protección de Datos (DPO) en funciones de supervisión y asesoramiento.
- Responsables de Recursos Humanos, únicamente cuando resulte necesario para proponer medidas disciplinarias.
- Servicios jurídicos, internos y/o externos cuando resulte necesario para la adopción de medidas legales o el ejercicio/defensa de reclamaciones.
- Proveedor del software/ plataforma del SII, como encargado del tratamiento actuando bajo instrucciones de EL COLEGIO y con deber de confidencialidad.

## **8. Transferencias internacionales**

No se prevén transferencias internacionales de datos. En caso de que algún proveedor implicase transferencia internacional, se adoptarán las garantías adecuadas conforme al RGPD y se informará debidamente.

## **9. Conservación**

Los datos del SII se conservarán únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación y, en todo caso, se suprimirán transcurridos tres (3) meses desde la recepción de la comunicación si no se hubieran iniciado actuaciones.

Excepcionalmente, podrán conservarse anonimizados exclusivamente como evidencia del correcto funcionamiento del sistema.

Si se iniciaran actuaciones (disciplinarias, administrativas o judiciales), los datos pertinentes se conservarán mientras sean necesarios para la tramitación y, posteriormente, durante los plazos de prescripción legal aplicables y/o mientras puedan derivarse responsabilidades.

## **10. Derechos de las personas interesadas**

Las personas interesadas pueden ejercitar los derechos de acceso, rectificación, supresión, limitación y oposición dirigiendo comunicación al DPO en la siguiente dirección [dpo@kensingtonschoolbcn.com](mailto:dpo@kensingtonschoolbcn.com), indicando el derecho que desean ejercitar.

El ejercicio de derechos podrá verse limitado cuando sea necesario para salvaguardar la confidencialidad de la investigación, proteger la identidad del informante y garantizar los derechos de terceros, conforme a la normativa aplicable (incluido el régimen específico de la Ley 2/2023 y las limitaciones del RGPD/LOPDGDD).

## **11. Delegado de Protección de Datos (DPD)**

Contactar con el DPO en [dpo@kensingtonschoolbcn.com](mailto:dpo@kensingtonschoolbcn.com), para consultas sobre protección de datos.

## **12. Reclamación**

si considera que el tratamiento de sus datos no se ajusta a la normativa de protección de datos, podrá presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

## **X. PROCEDIMIENTO DE INVESTIGACIÓN.**

El procedimiento de investigación se realizará conforme a lo establecido en el **Anexo II Protocolo de Investigaciones**.

#### **XI. VIGENCIA Y ACTUALIZACIÓN.**

La presente Política ha sido aprobada por el Órgano de Gobierno de EL COLEGIO

El texto de esta Política podrá ser revisado y actualizado, total o parcialmente, cuando así lo requieran circunstancias relevantes, tales como:

- a. Cambios legislativos que resulten de aplicación o tengan incidencia directa en la organización o en el propio documento.
- b. Recomendaciones o sugerencias realizadas, los miembros de la organización, o los distintos departamentos y unidades de EL COLEGIO.
- c. Otras situaciones que hagan necesaria su modificación.

Toda revisión o actualización que implique una alteración del contenido de la Política requerirá la aprobación del Órgano de Gobierno para su plena eficacia.

En Barcelona, a 05 de mayo de 2026.

## ANEXO I - MODELO DE COMUNICACIÓN

### Datos del Informante:

Nombre y apellidos:

Email:

Teléfono:

Domicilio/correo electrónico/lugar seguro a efectos de notificaciones (opcional):

### Datos sobre los hechos comunicados:

Tipo de Incumplimiento:

Email (si se conoce):

### Descripción detallada del Incumplimiento:

¿Cuándo?:

¿Dónde?:

¿Quién?:

¿Qué?:

### Cláusula protección de datos:

**Datos de contacto del Delegado de Protección de Datos.** [dpo@kensingtonschoolbcn.com](mailto:dpo@kensingtonschoolbcn.com)

**Finalidad:** Gestionar, tramitar y, en su caso, investigar las comunicaciones recibidas a través del SII, incluyendo la adopción de medidas internas y el seguimiento de actuaciones derivadas, en el marco de 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 información recibida se utilizará exclusivamente para las finalidades previstas en el marco del SII y con las garantías de confidencialidad establecidas.

**Legitimación:** El tratamiento es necesario para el cumplimiento de una obligación legal, conforme a la de la Ley 2/2023, de 20 de febrero (art. 6.1.c RGPD).

**Derechos:** Las personas interesadas pueden ejercitar los derechos de acceso, rectificación, supresión, y limitación y oposición de sus datos, dirigiendo comunicación al DPO en [dpo@kensingtonschoolbcn.com](mailto:dpo@kensingtonschoolbcn.com).

Le informamos que, si considera que el tratamiento de sus datos no se ajusta a la normativa de protección de datos, podrá presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

## **ANEXO II - PROTOCOLO DE INVESTIGACIONES**

### **1. OBJETO**

El presente protocolo regula el procedimiento a seguir desde la recepción de la comunicación hasta la inadmisión o la adopción de la resolución pertinente con las medidas que procedan incluyendo las actuaciones de instrucción encaminadas a comprobar la verosimilitud de los hechos relatados.

### **2. ALCANCE**

Este protocolo se aplica a todas las comunicaciones que se reciban en el Sistema Interno de Información de EL COLEGIO sobre acciones u omisiones que puedan constituir:

- Infracciones del Derecho de la Unión Europea, relativas a la protección sobre el informante, el funcionamiento de la Unión Europea o que incida en el mercado interior (competencia, subvenciones, ayudas y en materia fiscal).
- Infracciones penales.
- Infracciones administrativas graves o muy graves.
- Infracciones laborales en materia de seguridad y salud en el trabajo.
- Infracciones en materia de protección de datos

Y que afecten:

- Trabajadores por cuenta ajena.
- Autónomos.
- Accionistas, partícipes y miembros del órgano de administración, dirección o supervisión, (incluidos los miembros no ejecutivos).
- Trabajadores bajo supervisión y dirección de contratistas, subcontratistas o proveedores.
- Extrabajadores, voluntarios, becarios, candidatos, trabajadores en periodos de formación con independencia o personas en relación precontractual.
- Representantes de los trabajadores en funciones de asesoramiento y apoyo al informante.
- Personas vinculadas al informante, que le presten servicios o le asistan.

El canal podrá estar habilitado para la recepción de comunicaciones o informaciones fuera del ámbito anterior; en tal caso, dichas comunicaciones y sus remitentes quedarán fuera del ámbito de protección dispensado por la Ley 2/2023

### **3. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN.**

El responsable del Sistema Interno de Información será designado por el órgano de administración u órgano de gobierno de la entidad que corresponda.

El responsable del SII desarrollará sus funciones de forma independiente y autónoma respecto del resto de órganos de la organización, no pudiendo recibir instrucciones de ningún tipo en su ejercicio y debiendo disponer de los medios personales y materiales necesarios para llevarlas a cabo.

#### 4. GARANTÍAS PARA LA PERSONA INFORMANTE Y LA PERSONA AFECTADA.

##### Garantías para la persona informante:

- Protección frente a represalias, en los términos previstos en la normativa aplicable.
- Comunicación por los medios previstos en la Política del SII y sobre las materias del apartado 2.
- Acuse de recibo en un plazo máximo de siete (7) días desde su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.
- Tratamiento seguro y confidencial de la información, protección de identidades y datos personales, e impidiendo el acceso a personal no autorizado.
- Posibilidad de comunicación escrita, verbal o ambas, identificada o anónima.
- Plazo máximo de respuesta de tres (3) meses, con posibilidad de prórroga hasta un máximo de otros tres (3) meses adicionales, en caso de especial complejidad.
- Posibilidad de mantener la comunicación con el informante y solicitar información adicional cuando sea necesario.
- Respeto a derechos de protección de datos.
- Remisión al Ministerio Fiscal cuando los hechos pudieran ser constitutivos de delito o a la Fiscalía Europea si afectaran intereses financieros de la Unión Europea.

##### Garantías para la persona afectada:

- Respeto a la presunción de inocencia y al honor.
- Confidencialidad y reserva en la información y el proceso; obligación de secreto para todos los participantes.
- Derecho a ser informado (o no) sobre la marcha de la investigación siempre que no se comprometa la investigación y respetando el principio de confidencialidad.
- Información sucinta de los hechos atribuidos, salvaguardando la confidencialidad.
- Derecho a comparecer, declarar, aportar información o solicitar diligencias de prueba legales, oportunas y necesarias.
- Grabación de declaraciones o declaración escrita firmada, en caso de que así lo solicite.
- Acompañamiento por representante de trabajadores y abogado; derechos constitucionales (art. 24 CE: defensa, asistencia letrada, no autoincriminación).
- Respeto a derechos de protección de datos.

#### 5. PROCEDIMIENTO DE GESTIÓN.

##### a. Recepción de la comunicación

El responsable del Sistema Interno de Información actuará como receptor de las comunicaciones, asignará un ID único a la comunicación y, con carácter general, emitirá acuse de recibo en un plazo máximo **de siete (7) días** desde su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.

##### b. Análisis preliminar a la gestión de la comunicación de información

En un **plazo máximo de diez (10) días** desde el acuse de recibo el responsable del SII decidirá:

- Inadmitir la comunicación: Por falta de verosimilitud, ausencia de infracción (apartado 2), indicios de obtención delictiva de la información (remisión al Ministerio Fiscal), o reiteración sin nuevos elementos.
- Admitir en los **cinco (5) días** desde el acuse iniciando la investigación.
- Remitir inmediatamente al Ministerio Fiscal (en caso de hechos que puedan constituir delitos) o a la Fiscalía Europea (en caso de que los hechos afecten a los intereses financieros de la Unión Europea).
- Remitir al departamento competente para su tramitación.

#### **c. Investigación (Instrucción)**

La instrucción comprenderá las actuaciones encaminadas a comprobar la verosimilitud de los hechos relacionados, garantizando la confidencialidad e impidiendo el acceso de personal no autorizado.

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:

- El responsable del Sistema y a quien lo gestione directamente.
- El responsable de RRHH u órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias.
- El responsable de los servicios jurídicos, si procediera la adopción de medidas legales.
- Los encargados del tratamiento que eventualmente se designen.
- El delegado de protección de datos.
- La investigación será dirigida por el responsable del SII, que podrá designar un Instructor para la coordinación de actuaciones y custodia del expediente, bajo su supervisión.
- La participación del responsable de RRHH y/o de los servicios jurídicos solo se producirá cuando resulte necesaria y quedará documentada en el expediente con indicación del motivo, alcance y duración del acceso.

La investigación comenzará citando a la persona informante para ratificar la comunicación, ampliar información, proponer diligencias y medidas cautelares (plazo de **tres (3) días hábiles** para aportaciones). Se le informarán sus derechos, el procedimiento y la obligación de reserva de los hechos de los que pudiera tener conocimiento a fin de no alterar la investigación y proteger su figura de informante adecuadamente. Admitidas las diligencias, estas se practicarán en reuniones grabadas.

Se garantizará que la persona afectada tenga noticia de la comunicación y de los hechos relacionados de manera sucinta en el momento y forma adecuados para garantizar el buen fin de la investigación. Posteriormente, se citará a la persona afectada para exponer su versión y aportar prueba (en plazo de **tres (3) días hábiles**). En ningún caso se comunicará la identidad del informante ni se dará acceso a la comunicación.

#### **d. Resolución**

En el plazo máximo de tres (3) meses desde el acuse de recibo (o, si no se remitió acuse, desde el vencimiento del plazo de siete (7) días desde la comunicación), se emitirá resolución o, en

casos de especial complejidad, se acordará motivadamente la prórroga por un máximo de otros tres (3) meses adicionales.

Para la resolución del expediente, el Instructor, redactará un informe que deberá contener:

- Relación de antecedentes del caso.
- Resumen de las diligencias y pruebas practicadas.
- Los hechos que resulten acreditados.
- Las conclusiones.
- La propuesta de acciones y pautas de control.

La resolución se notificará al informante y a la persona afectada mediante un resumen adecuado que respete la confidencialidad, la protección de datos y, en particular, sin incluir información que pueda identificar al informante. Igualmente la resolución se elevará al Órgano de Gobierno, que decidirá sobre la adopción de las medidas organizativas o disciplinarias que procedan, limitando el contenido a la información imprescindible a dichos efectos.

**e. Seguimiento**

El responsable del SII supervisará el cumplimiento de las acciones y pautas adoptadas durante un mes tras la resolución.