P-11 SISTEMA INTERNO DE INFORMACIÓN

1. ALCANCE DEL SISTEMA DE INFORMACIÓN

El alcance del sistema interno de información viene establecido en la legislación aplicable, así como en los procedimientos del sistema de gestión de Hospitales Cosaga, donde se establece que podrá comunicarse:

a) Cualquier acción u omisión que pueda constituir una infracción del Derecho de Unión Europea que:
   - entren en el 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, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión,
   - o bien afecten a los intereses financieros de la Unión Europea tal y como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE);
   - o incidan en el mercado interior, tal y como se contempla en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión Europea en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades o con prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades.

b) Cualquier acción u omisión que pueda ser constitutiva de infracción penal o administrativa grave o muy grave conforme al derecho interno español.

c) Especialmente cualquier conducta tipificada en el Código Penal que pudieran dar lugar a la responsabilidad penal de las personas jurídicas recogidas en el Sistema de Gestión de Compliance Penal de Hospitales Cosaga.

d) Cualquier hecho o situación que pueda ser constitutiva de infracción o sanción administrativa contemplada en la normativa vigente en cada momento, y de forma particular, la infracción de la normativa reguladora de la prevención del blanqueo de capitales y financiación del terrorismo.

e) Cualquier infracción del Derecho laboral en materia de seguridad y salud en el trabajo, se entiende sin perjuicio de la establecida en su normativa específica.
f) Cualquier irregularidad (error material o fraude) cometida en el proceso de emisión de Información Financiera y contable de la Entidad.
g) Las violaciones del Código Ético y de Conducta de Hospitales Cosaga.

En adelante, el conjunto de disposiciones legales y directrices internas mencionadas cuya infracción es susceptible de ser denunciada a través del Sistema Interno de Información y sus Canales de Comunicación, serán denominadas como "la Normativa".

Las comunicaciones deberán hacer referencia a acciones u omisiones que Hospitales Cosaga tenga capacidad para investigar, corregir y reparar, es decir, relacionadas con las conductas de los miembros de Hospitales Cosaga o del resto de partes interesadas o socios de negocio que participan de las actividades, procesos y procedimientos de Hospitales Cosaga.

En cuanto al alcance personal, el SII ampara a todas las personas que informen sobre cualquier acción u omisión comprendida en el alcance material establecido en el apartado anterior, estableciendo un régimen de especial protección para las personas informantes contempladas en el art. 3 de la Ley 2/2023 que se desarrolla en este reglamento.

2. SISTEMA INTERNO DE INFORMACIÓN

El Órgano de Gobierno es el responsable de la implantación del Sistema interno de información y del tratamiento de los datos personales de conformidad con lo dispuesto en la normativa sobre protección de datos personales.

El Sistema interno de información debe ser el cauce preferente para informar sobre las acciones u omisiones previstas en el punto anterior, siempre que se pueda tratar de manera efectiva la infracción y si el denunciante considera que no hay riesgo de represalia.

2.1. REQUISITOS DE SISTEMA INTERNO DE INFORMACIÓN

El Sistema interno de información debe:

a) Permitir a las personas informantes y otros usuarios del SII comunicar información sobre las infracciones previstas en el punto 1 de este Reglamento, de acuerdo con los principios establecidos en Política del Sistema Integrado de Gestión y el Código Ético y de Conducta de Hospitales Cosaga.
b) Estar diseñado, establecido y gestionado de una forma segura, de modo que se garantice la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, y de las actuaciones que se desarrollen en la gestión y tramitación de esta, así como la protección de datos, impidiendo el acceso de personal no autorizado.
c) Facilitar la presentación de comunicaciones por escrito o verbalmente, o de ambos modos.
d) Integrar los distintos canales internos de información que pudieran establecerse dentro de la entidad.
e) Garantizar que las comunicaciones presentadas serán tratadas de manera efectiva, con el objetivo de investigar, corregir y reparar la posible irregularidad de la forma más inmediata.
f) Ser independiente el SII de cualquier otra organización y aparecer siempre diferenciado respecto al de otras entidades u organismos.
g) Contar con un responsable del sistema designado por el Órgano de Gobierno y que mantendrá el rol, funciones y responsabilidades recogidas en el punto 4 de este procedimiento.
h) Contar con un procedimiento general de gestión de las informaciones recibidas en los términos establecidos en el punto 6 de este procedimiento.
i) Establecer las garantías para la protección de los informantes y otros usuarios del SII y contar con procedimientos de protección a los informantes en los términos establecidos en el punto 8 de este procedimiento.
j) Contar con un Libro-Registro de Informaciones e Investigaciones bajo la custodia del Responsable del SII en los términos establecidos en el punto 4 de este procedimiento.
k) Ofrecer información adecuada, clara y fácilmente accesible, sobre los canales internos de información y los principios esenciales del procedimiento de gestión, que en todo caso estará accesible en la página web de la entidad, en una sección separada y fácilmente identificable.

3. DEFINICIÓN DE INFORMANTES Y OTROS USUARIOS DEL SISTEMA DE INFORMACIÓN

Hospitales Cosaga tiene dos grandes colectivos de usuarios del Sistema Interno de Información: consejeros, directivos y empleados y aquellos terceros que mantengan una relación contractual o comercial con las mismas, siendo los colectivos más relevantes proveedores, clientes y empresas subcontratadas.

Se integran en nuestro acervo normativo interno dos categorías diferenciadas de usuarios:

a) Los Informantes: termino que se recoge en la Ley 2/2023 y que identifica a las personas establecidas en su art. 3 cuando informan sobre infracciones contempladas en el art. 2 y aquellas otras personas de la organización que por razón de su cargo o función protegen, amparan o mantienen relaciones con las personas que hacen dichas comunicaciones. La característica principal de los Informantes es su derecho a recibir esta consideración por parte de las Autoridades Administrativas Independientes y disfrutar del régimen especial de protección establecido en la Ley 2/2023.
b) Otros usuarios del Sistema Interno de Información: que no pueden ser considerados informantes, tanto sea porque el contenido de la comunicación no está contemplado en el Art.2 de la Ley como porque la relación entre comunicante y Hospitales Cosaga no está contemplada en el art. 3 de la Ley.

4. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN

a) La función de Responsable del Sistema Interno de Información será desempeñada preferentemente por la persona que ocupe el cargo de Presidente de la Unidad de Cumplimiento Normativo (UCN) de la organización.
b) La designación del Responsable del Sistema Interno de Información deberá comunicarse a las Autoridades Administrativas Independientes competentes en los términos que se establezcan normativamente.
c) El Responsable del Sistema desarrollará sus funciones de forma independiente y autónoma respecto del Órgano de Gobierno y el resto de los órganos de la entidad, no recibirá instrucciones de ningún tipo en su ejercicio, y dispondrá de todos los medios personales y materiales necesarios para llevarlas a cabo.

d) El Responsable del Sistema podrá compatibilizar sus funciones con el desempeño ordinario de las funciones del puesto o cargo si se garantiza que no incurrirá en posibles situaciones de conflicto de intereses.
e) El Responsable del Sistema Interno de Información podrá elaborar, aprobar, comunicar y exigir el cumplimiento a todos los integrantes de Hospitales Cosaga de cuantos procedimientos, instrucciones, formatos resulten necesarios para desarrollar y aplicar eficazmente el presente Reglamento General del Sistema Interno de Información.
f) El Responsable del Sistema Interno de Información podrá apoyarse en los órganos de cumplimiento que dispone el Hospitales Cosaga para gestionar el SII y en especial podrá delegar en ellos la gestión de los canales internos y/o de los procedimientos de gestión de las informaciones con la finalidad de asegurar una gestión de los canales internos eficaz, independiente y ajena a cualquier conflicto de intereses.
g) Deberá mantener y custodiar un libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar, que no será público y recibirá el tratamiento de secreto empresarial, quedando restringido su acceso al Responsable del Sistema Interno de Información y a las personas que razonadamente designa y al que únicamente podrá accederse total o parcialmente para cumplir un requerimiento razonado de una Autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquella.
h) El Responsable del Sistema Interno de Información podrá proponer al Órgano de Gobierno la externalización de uno o todos los Canales Internos de Información o del procedimiento de recepción de informaciones cuando considere que esa es la mejor opción para asegurar la gestión eficaz e independiente de las comunicaciones o bien sea la opción que pueda generar más confianza en los usuarios e informantes.

El procedimiento de externalización deberá asegurar en todo caso:

a) Que el tercero externo ofrece garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones.

b) Que la gestión por un tercero no comportará pérdida de las garantías y requisitos establecidos en la Política de Información de Irregularidades y Protección de Informantes, ni una delegación de la responsabilidad sobre el Sistema Interno de Información en persona distinta del Responsable del Sistema Interno de Información.

c) La consideración del tercero externo como encargado del tratamiento a efectos de la legislación sobre protección de datos personales, suscribiéndose el 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.

5. CANALES INTERNOS DE INFORMACIÓN

a) El Sistema interno de información integrará todos los canales internos que permitan la presentación de comunicaciones sobre infracciones recogidas en el artículo 1 de este procedimiento.

b) El Sistema Interno de Información debe habilitar canales internos que permitan realizar comunicaciones verbales o por escrito, o de ambas formas.

c) Los usuarios de los canales internos deben ser informados de forma clara y accesible, sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

d) Los canales internos que se pongan a disposición de los usuarios e informantes deben facilitar que puedan indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones.

e) Los canales internos que permitan comunicaciones verbales, incluidas las realizadas a través de reunión presencial deberán documentar las comunicaciones, previo consentimiento del informante mediante una grabación de la conversación en un formato seguro, duradero y accesible, o a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla, ofreciendo al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

f) Los canales internos de información deben permitir la presentación y posterior tramitación de comunicaciones anónimas.

g) Los canales internos habilitados en Hospitales Cosaga por exigencia de normativas específicas, como son acoso sexual, laboral o por razón de sexo, Servicios de Atención al cliente o por normativa compliance se integrarán en el Sistema Interno de Información respetando los requisitos derivados de la normativa que los establece, resultando este Reglamento de aplicación supletoria en lo no regulado específicamente.

6. PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES

a) La aprobación del procedimiento de gestión de informaciones es una responsabilidad del Órgano de Gobierno que se cumple a través de este Procedimiento General del Sistema Interno de Información.
b) El Responsable del Sistema Interno de Información responderá de su tramitación diligente, asegurando el tratamiento adecuado de todas las comunicaciones recibidas.
c) El Sistema interno de información y los canales internos de información existentes deben cumplir con todos los requisitos establecidos en la ley 2/2023, así como las circulares o recomendaciones que pudieran publicar las Autoridades Administrativas Competentes.
d) Todos los canales internos de información que habilite Hospitales Cosaga quedarán sometidos a este procedimiento.
e) El procedimiento debe asegurar que se pondrá a disposición de todos los usuarios de los canales de denuncia internos información clara y accesible sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.
f) En el plazo de siete días naturales siguientes a la recepción de cualquier comunicación deberá acusarse recibo al informante, excepto en el supuesto que -por las características del canal, de la comunicación o por cualquier otra circunstancia- el Responsable del SII o los gestores del canal consideren que el acuse de recibo pone en peligro la confidencialidad de la comunicación.
g) Todas las comunicaciones recibidas deberán ser objeto de un análisis preliminar para determinar si su contenido está comprendido en el punto. 2 de este procedimiento y si procede o no procede su admisión según los criterios establecidos en la legislación vigente y en este Reglamento, acordándose el archivo a la mayor brevedad cuando corresponda.

h) Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento que se tenga constancia de ello, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se conservara durante el tiempo en que se tramite el procedimiento judicial.

i) Si la comunicación recibida no estuviera relacionada con acciones u omisiones que Hospitales Cosaga tenga capacidad para investigar, corregir y reparar, es decir, informaciones no relacionadas con las conductas de los miembros de Hospitales Cosaga o del resto de partes interesadas o socios de negocio que participan de las actividades, procesos y procedimientos de Hospitales Cosaga, deberá inadmitirse, indicando al informante los canales internos y externos que pudieran resultar más adecuados para formular su comunicación.

j) En el momento de admitir una comunicación se deberá establecer el nivel de protección que se debe asignar al informante conforme al punto 7 de este procedimiento.

k) El procedimiento de instrucción tiene como finalidad realizar las actuaciones imprescindibles para determinar la naturaleza de los hechos informados y adoptar una resolución que podrá ser:

- De archivo de las actuaciones.
- De remisión al órgano interno competente por la naturaleza de los hechos objeto de comunicación.
- De remisión al Ministerio Fiscal o a la Fiscalía Europea, si procede.

l) El procedimiento de instrucción deberá tramitarse con la mayor celeridad y 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, tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación.

m) En supuestos excepcionales y de especial complejidad se podrá extender el plazo por un periodo máximo de otros tres meses adicionales.

n) Todos los canales de comunicación interna que se implanten deben tener mecanismos que permitan mantener la comunicación con el informante y, si se considera necesario, solicitarle información adicional.

o) El procedimiento de comunicaciones, y en general el Sistema Interno de Información, debe garantizar que cuando la comunicación sea remitida por canales de denuncia que no sean los establecidos o llegue primero a miembros

del personal no responsable de su tratamiento la comunicación será remitida inmediatamente al Responsable del Sistema.

p) El procedimiento debe respetar todas las disposiciones sobre protección de datos personales aplicables de acuerdo con el título VI de la Ley 2/2023 de Protección de Datos y Garantía de Derechos Digitales, y el RGPD.

q) Se faculta al Responsable del Sistema Interno de Información para elaborar y publicar cuantos procedimientos, instrucciones o formatos resulten necesarios para asegurar el cumplimiento de todos los requisitos legales, de este Reglamento y de la Política en que se fundamenta.

7. PROTECCIÓN DE LOS DENUNCIANTES.

7.1. PROHIBICIÓN DE LAS REPRESALIAS Y PROTECCIÓN DE LOS INFORMANTES Y PERSONAS USUARIAS DE LOS CANALES INTERNOS

a) Queda terminantemente prohibido cualquier acto que pueda considerarse represalia, incluidas las amenazas de represalia y las tentativas de represalia, contra las personas que presenten cualquier comunicación conforme a lo previsto en el Código Ético y de Conducta y en este procedimiento.

b) Los actos que tengan por objeto impedir o dificultar la presentación de comunicaciones y revelaciones, así como los que constituyan represalia o causen discriminación tras la presentación de aquellas al amparo de este procedimiento, son nulos de pleno derecho y darán lugar a medidas correctoras disciplinarias o de responsabilidad para los directivos, empleados u otras personas de la organización que las comentan, sin perjuicio de su comunicación a la autoridad administrativa competente para la imposición de las correspondientes sanciones.

c) Se entiende por represalia todo comportamiento, acción u omisión prohibido por la ley, o que, de forma directa o indirecta, conlleve un trato desfavorable que sitúe a las personas que los sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, como consecuencia de su condición de informantes, o por haber usado los canales de comunicación internos o haber realizado una revelación pública.

d) El Responsable del SII podrá desarrollar instrucciones estableciendo criterios o directrices interpretativas sobre aquellas conductas que puedan comportar un riesgo de ser consideradas como represalias.

e) La protección de los usuarios de los canales de comunicación y de los Informantes definidos en el punto 4 de este procedimiento se aplicará desde el momento del triaje inicial y admisión de su comunicación y se regirá por los siguientes criterios:

   a. El Responsable del SII asegurará la comunicación constante y fluida con el informante o usuario del canal de comunicación con la finalidad de conocer en todo momento si ha sufrido algún tipo de represalia o consecuencia tras haber realizado la comunicación.

   b. Se le ofrecerá soporte y asesoramiento sobre las consecuencias de su comunicación informándoseles especialmente sobre la protección que les ofrecen las Autoridades de Protección al Informante competentes y sobre los canales externos de información.

7.2. RECONOCIMIENTO Y ACCESO AL RÉGIMEN DE PROTECCIÓN DE LOS INFORMANTES Y USUARIOS DE LOS CANALES INTERNOS

a) Todos los usuarios del Sistema Interno de Información de Hospitales Cosaga tienen derecho a la salvaguarda y confidencialidad establecidas en el Código Ético y de Conducta y en este procedimiento.

b) Las personas Informantes definidas en el punto 4 de este procedimiento tendrán derecho al régimen de protección especial previsto en la Ley 2/2023.

c) Las personas que hayan informado de forma anónima pero que posteriormente hayan sido identificadas y cumplan las condiciones previstas en este procedimiento, tendrán derecho a la protección especial establecida en el mismo.

8. PROTECCIÓN DE DATOS PERSONALES

El tratamiento de datos de carácter personal en el Sistema Interno de Información atenderá en todo caso a lo previsto en la normativa de Protección de Datos de Carácter Personal, y específicamente a lo establecido en la LOPDGDD 3/2018 y RGPD 2016/679.

6 CONTROL DE CAMBIOS Y MODIFICACIONES

DATA	EDICIÓN	NATURALEZA DO CAMBIO
19/01/2024	01	PRIMER EJEMPLAR