



**PROTOCOLO DEL CANAL INTERNO DE INFORMACIÓN DEL HOSPITAL
UNIVERSITARIO SAN FRANCISCO DE ASIS DE CONFORMIDAD A 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.**



CONTROL DE APROBACIÓN

Versión	Fecha	Descripción acción	Páginas	Autor	Fecha de aprobación	Firma del responsable
V.01	13/06/2023	Creación del documento	Todas	DLA		

Este documento es privado y confidencial, para uso exclusivo del Cliente. Queda prohibida cualquier forma de reproducción sin autorización escrita del **Despacho De Lorenzo Abogados**.

De Lorenzo Abogados, no asume ninguna responsabilidad por problemas legales o técnicos causados por el incumplimiento por parte del Cliente de las recomendaciones realizadas.

ÍNDICE

1. OBJETO.....	5
2. MARCO NORMATIVO Y TEXTOS DE REFERENCIA.	5
3. ÁMBITO DE APLICACIÓN.	6
4. COMITÉ DE LOS CANALES DE COMUNICACIÓN INTERNOS DE INFORMACIÓN.....	6
5. FUNCIONAMIENTO DE LOS SISTEMAS INTERNOS DE INFORMACIÓN	8
6. PROCEDIMIENTO PARA LA TRAMITACIÓN E INVESTIGACIÓN DE LAS INFORMACIONES.	12
7. EXTERNALIZACIÓN DE LOS CANALES INTERNOS DE INFORMACIÓN	15
8. ¿QUIÉN PUEDE INFORMAR?	17
9. ¿QUÉ CONDUCTAS PUEDEN INFORMARSE A TRAVÉS DEL CANAL?	17
10. GARANTÍAS Y MEDIDAS DE PROTECCIÓN.....	18
11. CONFLICTOS DE INTERESES.	22
12. CANAL EXTERNO DE LA AUTORIDAD INDEPENDIENTE DE PROTECCIÓN AL INFORMANTE.....	22
13. DIFUSIÓN Y ENTRADA EN VIGOR.	23



HISTÓRICO

Versión	Fecha	Descripción acción	Páginas	Responsable

1. OBJETO

El objeto del presente Protocolo es establecer unas pautas sobre la creación del **canal interno de información** dentro del grupo, adecuar el funcionamiento de los mismos, y la gestión de la investigación de los hechos informados, de conformidad con 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.

El **canal interno de información** es el cauce preferente,- para trabajadores, clientes, proveedores y otros-, para informar sobre aquellas acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave, todo ello en los términos previstos 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, teniendo en cuenta los requisitos establecidos en la directiva (UE) 2019/1937 relativa a las personas que informen sobre infracciones del Derecho de la unión.

Además de las citadas normas, la implementación del canal debe integrarse a otras normativas nacionales e internacionales, tales como la laboral, protección de datos, normas de igualdad de género, etc. La implantación de estos canales tiene como **finalidad** los siguientes objetivos:

- **Integrar** los distintos canales internos de información dentro de la organización.
- Ayudar a **detectar** las irregularidades que se puedan cometer dentro de la organización, lo que permite **implementar** las medidas correctoras que procedan a efectos de prevenir su reiteración.
- **Afianzar** la **cultura de cumplimiento** y **buenas prácticas** de la corporación.
- **Dotar** a la organización de **mecanismos de conocimiento** para la implantación o modificación de controles en relación con las eventuales conductas de incumplimiento.
- **Garantizar** que las comunicaciones presentadas se traten de forma efectiva, siguiendo los principios recogidos en la **Política del sistema interno de información** y conforme a las pautas establecidas en el **Protocolo de gestión** de las informaciones recibidas.

2. MARCO NORMATIVO Y TEXTOS DE REFERENCIA.

Las referencias tenidas en cuenta para la redacción de este Procedimiento han sido:

- 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.

- 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.
- Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres.
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Circular 1/2016, de 22 de enero, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Norma ISO 37002:2021, sobre sistemas de gestión de denuncias.

3. ÁMBITO DE APLICACIÓN.

El presente documento es de aplicación para el HOSPITAL UNIVERSITARIO SAN FRANCISCO DE ASIS, en adelanta HUSFDA, y para todas sus empresas vinculadas.

4. COMITÉ DEL CANAL INTERNO DE INFORMACIÓN

El comité de dirección de HUSFDA de conformidad con lo exigido 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, tiene encomendada la responsabilidad de la implantación de estos sistemas internos de información:

1. El órgano de administración u órgano de gobierno de cada entidad u organismo obligado por esta ley será el responsable de la implantación del Sistema interno de información, previa consulta con la representación legal de las personas trabajadoras, y tendrá la condición de responsable del tratamiento de los datos personales de conformidad con lo dispuesto en la normativa sobre protección de datos personales¹.

En este sentido, el comité dirección ha acordado constituir -en comité de dirección celebrado el 12/06/2023-, un Comité “del canal interno de información”, el Comité realizará sus funciones en todos los canales establecidos dentro de HUSFDA, siendo las siguientes:

¹ Artículo 5.1 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.

El Comité se encargará:

1. Del diseño y la implantación del canal interno de información de conformidad a los requisitos establecidos 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. De la verificación y puesta en marcha del sistema interno;
3. De facilitar la formación para conocer el acceso y el funcionamiento del canal a través de formación que se podrá ofrecer online o presencial a todo el personal.

El Comité se comprometerá:

1. A la entrega del Procedimiento del canal de comunicación interno de a todos los trabajadores del mismo modo, se encargará de facilitar el acceso del mismo a proveedores, clientes o tercero, a través de publicidad en las distintas páginas web del grupo;
2. A realizar reuniones de seguimiento periódicas para comprobar la efectividad y el buen funcionamiento del canal de comunicación interno;
3. A la elaboración y entrega de informes sobre los registros y actuaciones realizadas con carácter semestral;
4. A establecer una Política propia del Canal y establecer un Procedimiento de gestión del mismo;
5. A la realización de una auditoría anual del funcionamiento del canal de la que deberá informar y reportar al Consejo de Administración, y al Responsable del Sistema interno.

En este sentido, se ha considerado adecuado por el Consejo de Administración que este Comité sea constituido como un **órgano colegiado**, y que únicamente estará compuesto por las personas físicas que pueden tener acceso a los datos de estos sistemas internos - de conformidad con lo establecido en el artículo 32 de la ley -, tratando de proteger lo máximo posible la sensibilidad de la información recibida en estos canales.

En este Comité habrá un **Responsable del Sistema**, que deberá ser la persona que dentro de la Organización tenga encomendadas las funciones de implementar políticas de *Compliance*, y que debe ser un directivo de la entidad que ejercerá su cargo con independencia del Órgano de Administración, en el caso de ya exista una persona responsable de la función de cumplimiento normativo o de política de integridad, esta persona podrá ser designada como Responsable del Sistema siempre que cumpla con los requisitos establecidos en la ley.

El Comité que velará por el efectivo funcionamiento del canal reportando al Consejo de Administración, fomentará el fortalecimiento de la cultura de la información, de las infraestructuras de integridad de la Organización y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público.

El Responsable del canal interno de información desarrollará sus funciones de forma independiente y autónoma del resto de órganos de la Entidad.

El Responsable del canal no recibe instrucción alguna en el desarrollo de su actividad por parte del resto de órganos de la entidad y dispone de todos los recursos necesarios para dar cumplimiento a la Política del canal interno de información y al Protocolo del canal interno de información, que, entre otros, cuenta con la colaboración de un proveedor externo: DE LORENZO ABOGADOS, S.L.P., en delante De Lorenzo Abogados, que garantiza la independencia e imparcialidad en el tratamiento de la información facilitada, y evita cualquier tipo de conflicto de interés con otros miembros de la entidad.

5. FUNCIONAMIENTO DEL SISTEMA DEL CANAL INTERNO DE INFORMACIÓN

El funcionamiento de los sistemas internos de información se establecerá de la siguiente forma:

1. El informante/es que quieran notificar alguna infracción de las establecidas 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 podrán hacerlo accediendo a la página web del HOSPITAL UNIVERSITARIO SAN FRANCISCO DE ASIS. A través de un link donde podrá **“Acceso canal interno de información”** se abrirá una página donde se explicará en que consiste el canal y cuál es su finalidad. El canal estará accesible y visible en la página web garantizando la accesibilidad al mismo.
2. Una vez que se active el link se abrirá una pestaña que dará traslado al informante al cuestionario que deben cumplimentar y que será enviado al gestor externo.

INTRODUCCIÓN

➔ **HOSPITAL UNIVERSITARIO SAN FRANCISCO DE ASIS**, en adelante **HOSPITAL SAN FRANCISCO DE ASIS**, ha implementado un canal interno de comunicación dentro del grupo de conformidad con la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informan sobre infracciones normativas y de lucha contra la corrupción.

El canal de comunicación interno de comunicación es el cauce preferente -para trabajadores, clientes, proveedores y otros-, para informar sobre aquellas acciones u omisiones que pueden ser constitutivas de infracción penal o administrativa grave o muy grave.

Debemos reseñar que **HOSPITAL SAN FRANCISCO DE ASIS** ofrece la posibilidad de que el informante cumplimente el formulario de forma anónima, es decir, sin tener que cumplimentar ningún dato de identificación. En ese caso, vas a recibir un código único y una URL una vez completa el formulario. Por favor, guarda ese acceso para poder consultar en todo momento el estado y resolución de tu comunicación.

El objetivo la implantación de dicho canal de comunicación interno viene enmarcado en la consolidación de la continua mejora de la sociedad **HOSPITAL SAN FRANCISCO DE ASIS**, en el alineamiento con las buenas prácticas corporativas y en la generación de instrumentos que mitiguen el riesgo de la comisión de y/o delitos de sanciones administrativas.

El canal interno será externalizado con el fin de garantizar la máxima confidencialidad, independencia e imparcialidad de las informaciones recibidas. Puede acceder a la Política de Privacidad en el apartado documentos adjuntos para saber más sobre el tratamiento realizado sobre sus datos personales.

Del mismo modo, **HOSPITAL SAN FRANCISCO DE ASIS** pone a disposición de todos los informantes un protocolo de funcionamiento del canal interno de comunicación donde podrán consultar cualquier duda.

Cualquier persona que realice una actuación que suponga una efectiva limitación de los derechos y garantías previstas en esta ley, realice a través de contratos o acuerdos a nivel individual o colectivo y en general cualquier intento o acción efectiva de impedir la presentación de comunicaciones o impedir, frustrar o ralentizar su seguimiento, incluida la aportación de información o documentación falsa por parte de los requeridos para ello, se someterá a los procedimientos y sanciones disciplinarias que correspondan de acuerdo con la legislación laboral vigente en cada momento y el convenio colectivo que resulte de aplicación.

Relación con la organización *



Tipología de la conducta a comunicar conforme a la Ley 2/2023 *



Busca un valor ...



- Contratación pública
- Servicios, productos y mercados financieros
- Blanqueo de capitales o financiación del terrorismo
- Seguridad y conformidad de los productos comercializados
- Seguridad del transporte
- Protección del medio ambiente
- Protección frente a radiaciones y seguridad nuclear
- Seguridad de los alimentos y los piensos, la sanidad animal y bienestar de los animales

¿Desea que la comunicación sea anónima?



Nombre y Apellidos



Email



Teléfono



Descripción de la infracción *



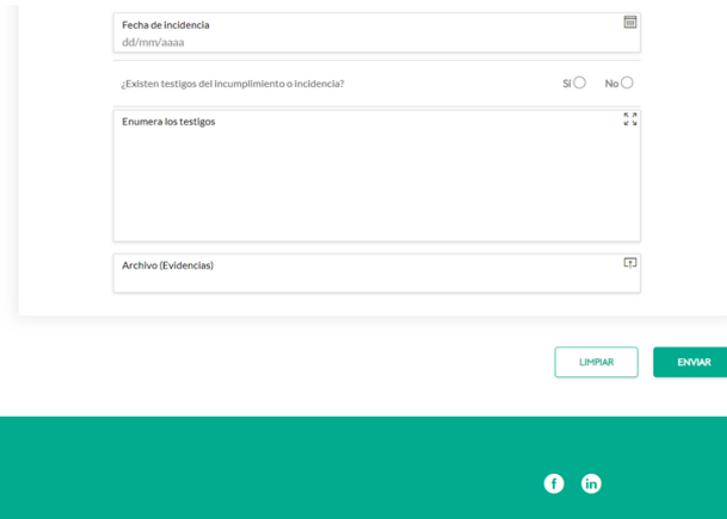
Fecha de incidencia



dd/mm/aaaa

¿Existen testigos del incumplimiento o incidencia?

Sí No



Fecha de incidencia
dd/mm/aaaa

¿Existen testigos del incumplimiento o incidencia? Sí No

Enumera los testigos

Archivo (Evidencias)

LIMPIAR ENVIAR

Hospital Universitario San Francisco de Asís

f in

3. El informante tendrá que cumplimentar de forma obligatoria (*) los siguientes apartados:

- **Relación con la organización:** persona interna o externa.
- **Tipología de la conducta** de conformidad a 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 este sentido el informante, tendrá la opción de seleccionar la conducta ilícita que considere, o tendrá la opción de seleccionar infracción administrativa.
- **Sobre el anonimato en la información.** El informante tendrá la opción de hacer la notificación de forma anónima (sin que en ningún momento aparezcan sus datos de identificación, ni tan siquiera hay que añadir dirección de correo electrónico) o por el contrario haciendo la notificación aportando los datos de identificación del informante para lo que habrá que añadir apellidos, y nombre, número de teléfono, correo electrónico...).
- **Descripción de la información.** El informante podrá desarrollar la descripción de lo sucedido. Para iniciar una investigación sobre la información, el gestor deberá tener una mínima información sobre lo sucedido, de forma contraria no podría iniciarse ninguna investigación. Para el correcto desarrollo de la investigación será de gran ayuda que el informante pueda señalar el centro en el que han ocurrido los hechos.
- **Fecha de la incidencia.** El informante podrá indicar la fecha en la que sucedieron los hechos.
- **Testigos.** El formulario establece un apartado para indicar si hay testigos o no de los hechos sucedidos. Si el informante indica que si hay testigos deberá identificarlos.

- **Archivo (Evidencia).** En este apartado el informante podrá subir a la página cualquier archivo o documentación que entienda procedente y/o de utilidad para la investigación.

4. Una vez el informante haya podido cumplimentar debidamente el formulario y enviado, se creará un código que será **único e intransferible** y al que solo tendrá acceso el informante.

5. El código numérico que se asigna a cada informante tras cumplimentar el formulario servirá para que posteriormente el informante pueda consultar el estado de la tramitación de la investigación, y para hacer cualquier comunicación adicional.



Se han enviado correctamente los datos.
Puedes seguir su tramitación en el siguiente enlace. No olvides guardar el código de acceso, lo necesitarás para acceder al enlace de seguimiento.

601460

COPIAR ENLACE DE SEGUIMIENTO



6. Si el informante extravía o pierde el número de seguimiento asignado a su formulario, ni el gestor, ni el usuario podrán recuperar el número de seguimiento, en este sentido, el objetivo es proteger lo máximo posible la confidencialidad del informante. Si esto sucediese el informante tendrá que cumplimentar un nuevo formulario. En consecuencia, **recalcamos la importancia de conservar tanto el código como el enlace de seguimiento**, dado que, sin ellos, el informante anónimo no podrá acceder al expediente, lo que puede conllevar a su archivo en caso de no evacuar algún requerimiento que se le pueda efectuar mediante el mismo.

6. PROCEDIMIENTO PARA LA TRAMITACIÓN E INVESTIGACIÓN DE LAS INFORMACIONES.

La gestión de las comunicaciones recibidas se desarrolla y divide en las siguientes fases:

1. Fase previa: Esta fase está detallada y desarrollada en el apartado anterior. El informante tendrá que acceder al link del canal interno de información cuando quiera informar de alguna conducta de las recogidas en este manual.

2. Fase inicial: Esta fase se iniciará una vez el informante envíe correctamente cumplimentado el formulario con los datos, y obtenga un código de seguimiento, cuando la comunicación sea anónima, o bien, si la comunicación no ha sido anónima, haya recibido en su correo electrónico para realizar el seguimiento.

3. Fase de recepción de la información. En esta fase, el gestor del sistema confirmará la correcta recepción de la información (acuse de recibo). En esta misma fase, se podrá solicitar información adicional y/o documentación que se considere relevante para la clasificación y tramitación de la misma.

Dicha recepción se llevará a cabo en el **plazo máximo de 7 días naturales.**

Con el fin de poder admitir y tramitar la información recibida, resultará necesario que, en el apartado de descripción de la infracción, se haga una exposición de los hechos, lo más detallada posible, a saber:

1. Los hechos acaecidos (lugar, duración y fecha).
2. La posible infracción cometida.
3. El responsable.
4. Datos de posibles testigos, así se adjunte la documentación necesaria o propicia para la resolución de la comunicación.

Los informantes podrán seguir el proceso de gestión de su comunicación en todo momento dependiendo de la formalidad en la que hayan establecido su forma de notificar la información:

- **De forma anónima:** a través del enlace que se le facilitó cuando se registró la comunicación, junto al código de acceso a la misma.
- **Con datos de identificación:** a través del vínculo enviado a aquellos informantes que hayan facilitado su correo electrónico.

4. Fase de admisión de la información.

En esta fase, el gestor del sistema, llevará a cabo un análisis preliminar mediante el cual se validará o no la comunicación efectuada, dependiendo de si la misma resulta o no admisible.

Se **inadmitirá** toda aquella comunicación que:

1. Carezca de datos necesarios para la verificación de la infracción comunicada.

2. Carezca de objeto, esto es, que no responda a ningún tipo de infracción susceptible de comunicación a través del Canal interno de información.
3. Carezca de verosimilitud.
4. Carezca manifiestamente de fundamento.
5. Carezca de información nueva con respecto a otra comunicación resuelta anteriormente por los mismos hechos.

5. Fase de la Instrucción de la información.

Validada la comunicación, se recabará la información y/o documentación que precise, realizando un exhaustivo análisis de los datos recogidos para comprobar la certeza y verosimilitud de los hechos comunicados y la concurrencia de infracción o no derivada de los mismos, asegurándose en todo momento de preservar el anonimato del informante.

Tras la evaluación inicial de la comunicación y determinándose que los hechos indicados son susceptibles de investigación, se tomarían una o más de las siguientes acciones:

1. Involucrar a Áreas (por ejemplo, recursos humanos, legal, auditoría interna, compliance, salud y seguridad, finanzas), si es necesario, y si esto no compromete la confianza, imparcialidad y protección de la investigación, para apoyar la investigación.
2. Recopilar más información.
3. Tomar medidas preliminares (por ejemplo, aseguramiento de pruebas, prestar asesoramiento e información completos, independientes, de fácil acceso y gratuitos, sobre los procedimientos y recursos disponibles, así como sus derechos).
4. Tomar medidas de protección al Informante.
5. Investigar la comunicación de irregularidades.
6. Informar en su caso a las autoridades pertinentes (por ejemplo, organismo regulador o de aplicación de la ley) garantizando en todo momento la defensa del HOSPITAL UNIVERSITARIO SAN FRANCISCO DE ASIS.

Durante todo el proceso de investigación e instrucción deben **garantizarse los siguientes principios**:

- Garantizar los derechos de los involucrados, como pueden ser el derecho a la presunción de inocencia, el derecho al honor y la reputación, el derecho al debido proceso y a la defensa entre otros.
- No deberá interferir directa o indirectamente con una investigación judicial. Debería cooperar cuando sea apropiado o requerido.
- Deberá asegurar y proteger las pruebas.
- Los datos personales deberían gestionarse de acuerdo con el apartado 7.5.4 (Protección de Datos).
- Debería proteger cualquier información que pueda identificar a cualquier sujeto de la información.

- Deberían poder escalarse y adaptarse a medida que las circunstancias puedan cambiar según avance la investigación.

El Responsable del Sistema es el encargado de que la investigación se realice correctamente, delegando la gestión de la misma en un “instructor” que será un experto externo, De Lorenzo Abogados, quien se encargará de la gestión del sistema. En este sentido, De Lorenzo Abogados firmará un acuerdo de confidencialidad respecto a la información y documentación a la que tengan acceso con motivo de la investigación de los hechos.

El Instructor tendrá acceso a toda la documentación e información relacionada con la comunicación. Si fuese necesario, teniendo especialmente en cuenta la gravedad de los hechos, el Instructor propondrán al Comité la adopción de medidas cautelares a fin de proteger al informante y/o evitar la reiteración en el comportamiento irregular. Las medidas deben estar justificadas, motivadas y ser proporcionales.

El Instructor podrá involucrar a otras áreas o departamentos que puedan ayudar al Responsable del Canal de Comunicación en las actuaciones necesarias en el marco de la investigación.

El Instructor llevará a cabo las diligencias de investigación que, a su juicio, resulten necesarias para comprobar la veracidad de los hechos informados. Tales diligencias se regirán por los siguientes **principios** que deberán ser observados en todo momento:

- a. Proporcionalidad:** los datos e información recopilados durante la investigación se limitarán a los estricta y objetivamente necesarios para comprobar la realidad de los hechos comunicados.
- b. Garantía de confidencialidad y protección de la intimidad y la dignidad de las personas implicadas:** todas las comunicaciones recibidas se tratarán de forma confidencial y de conformidad con la normativa de protección de datos en vigor, respetando el Derecho al honor e intimidad personal y familiar.
- c. Investigación exhaustiva de los hechos, objetiva e imparcial:** Las comunicaciones admitidas a trámite serán investigadas siempre de manera imparcial, íntegra, objetiva, independiente y honesta por parte del Instructor.
- d. Igualdad entre las partes:** se evitarán situaciones injustas de privilegio de una de las partes (informante o investigado) en perjuicio de la otra.
- e. Derecho de contradicción:** derecho de las partes -informante e investigado- a fin de hacer valer sus respectivas pretensiones y a ser oído.

Toda persona con conocimiento de una comunicación está obligada a colaborar lealmente con la investigación y a guardar secreto sobre su contenido.

Durante la fase de instrucción, se facilitará la posibilidad de comunicación continua con el informante, y se informará a la persona afectada sobre la existencia de la información recibida, los hechos que se le atribuyen, su derecho a presentar alegaciones por escrito, así como cualquier medio de prueba que considere pertinente, haciéndole igualmente entrega de la cláusula informativa del tratamiento de sus datos personales.

El plazo máximo para dar respuesta a las actuaciones de investigación no podrá superar los **tres meses desde el acuse de recibo de la comunicación**, pudiéndose ampliar dicho plazo por otros tres meses más únicamente en casos de especial complejidad. No obstante, HUSFDA se compromete a no dilatar la investigación más de lo estrictamente necesario.

6. Resolución de la información.

Concluida la fase de instrucción, se emitirá un **informe y propuesta de resolución** donde se recogerá una breve descripción de los hechos objeto de la información, las actuaciones llevadas a cabo durante la investigación de los mismos, y las conclusiones alcanzadas.

La resolución bien acordará el archivo de las actuaciones, o bien acordará la adopción de algún tipo de medida sancionatoria frente al responsable, así como la remisión al Ministerio Fiscal o la autoridad competente cuando así proceda.

El Responsable del Sistema emitirá un **informe de cierre** de la comunicación que contendrá entre otras informaciones las siguientes:

1. Una exposición de los hechos relatados junto con el código de identificación de la comunicación y la fecha de registro.
2. La clasificación de la comunicación a efectos de conocer su prioridad o no en su tramitación.
3. Las actuaciones realizadas con el fin de comprobar la verosimilitud de los hechos.
4. Las conclusiones alcanzadas en la instrucción y la valoración de las diligencias y de los indicios que las sustentan.

El plazo para finalizar las actuaciones e informar tanto al informante como a la persona afectada, será de **tres meses desde** la recepción de la información, salvo que se haya prorrogado la instrucción en aquellos casos de especial complejidad.

Una vez concluida la tramitación se procederá a su archivo en el **Libro Registro**.

7. EXTERNALIZACIÓN DEL CANAL INTERNO DE INFORMACIÓN

El artículo 6 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 establece la posibilidad de externalización de esos canales internos de comunicación. El Comité de dirección de HUSFDA ha decidido encomendar esta función a la Firma Legal De Lorenzo Abogados con el fin de ofrecer mayores niveles de independencia y confidencialidad. En este sentido, De Lorenzo Abogados, se encargará de la gestión del canal interno.

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

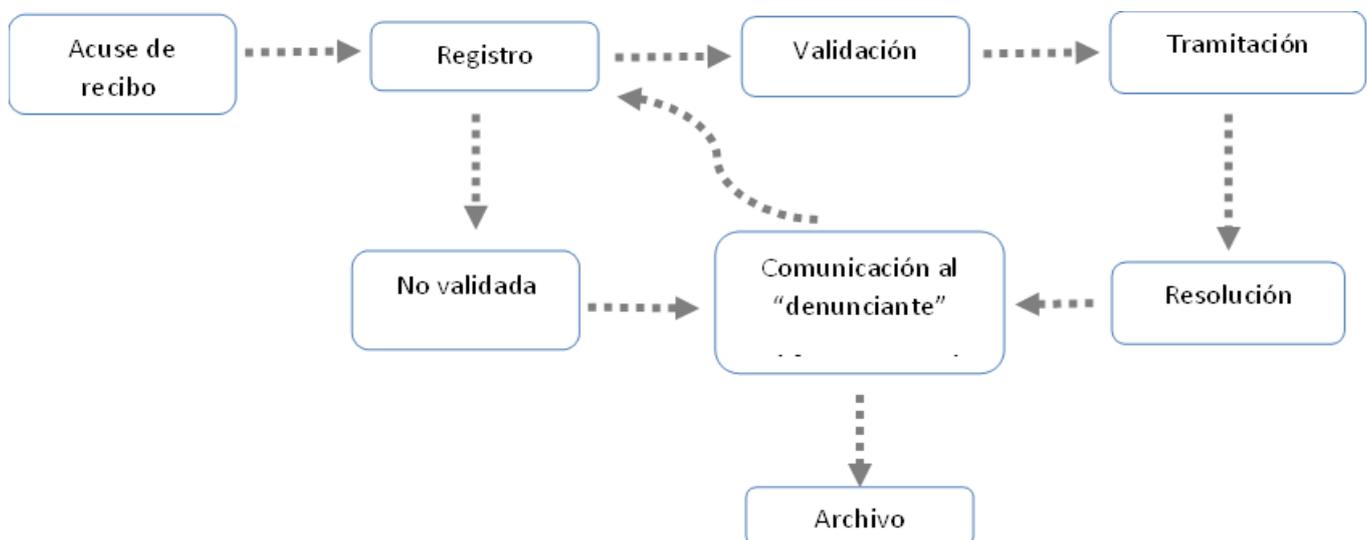
2. La gestión del sistema por un tercero externo exigirá en todo caso que este ofrezca garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones. La existencia de corresponsables del tratamiento de datos personales requiere la previa suscripción del acuerdo regulado en el artículo 26 del Reglamento (UE) 2016/679

del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

3. La gestión del Sistema interno de información por un tercero no podrá suponer un menoscabo de las garantías y requisitos que para dicho sistema establece esta ley ni una atribución de la responsabilidad sobre el mismo en persona distinta del Responsable del Sistema previsto en el artículo 8. 4. El tercero externo que gestione el Sistema tendrá la consideración de encargado del tratamiento a efectos de la legislación sobre protección de datos personales. El tratamiento se registrará por el acto o contrato al que se refiere el artículo 28.3 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016².

En este caso, la externalización de la gestión de los canales consistiría en que un tercero externo, a HUSFDA de conformidad a los requisitos establecidos en la ley se hará cargo de la gestión del mismo.

1. La gestión será encargada a - DE LORENZO ABOGADOS, S.L.P-, quien se encargará de la la recepción, recopilación, el procesamiento, y la investigación de las comunicaciones recibidas. Siguiendo el siguiente **esquema de funcionamiento**:



² Artículo 6 de 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. La gestión de los sistemas internos de información se hará, a través de un software de la mercantil Lefebvre cuyo nombre es “centinela”. Sobre la posibilidad de externalizar estos canales se pronuncia la Fiscalía General del Estado en la Circular 1/2015:

“Tampoco existe inconveniente alguno en que una gran compañía pueda recurrir a la contratación externa de las distintas actividades que la función de cumplimiento normativo implica. Carecería de sentido y restaría eficacia al modelo imponer a una multinacional la realización y control interno de todas las tareas que integran la función de cumplimiento normativo. Lo verdaderamente relevante a los efectos que nos ocupan es que la persona jurídica tenga un órgano responsable de la función de cumplimiento normativo, no que todas y cada una de las tareas que integran dicha función sean desempeñadas por ese órgano. Muchas de ellas incluso resultarán tanto más eficaces cuanto mayor sea su nivel de externalización, como ocurre por ejemplo con la formación de directivos y empleados o con los canales de denuncias, más utilizados y efectivos cuando son gestionados por una empresa externa, que puede garantizar mayores niveles de independencia y confidencialidad.”

3. La gestión del sistema interno de información por un tercero no podrá suponer un menoscabo de las garantías y requisitos que para dicho sistema establece la ley ni una atribución de la responsabilidad sobre el mismo en persona distinta del responsable del sistema.

4. El gestor externo también se encargará de la formación que la empresa deberá ofrecer a todos los trabajadores para informar de la existencia y funcionamiento de estos canales. Del mismo modo, se encargará de realizar las auditorias anuales para comprobar el correcto funcionamiento del canal.

8. ¿QUIÉN PUEDE INFORMAR?

Cualquier persona o grupo de personas vinculados o afectados por la actividad HUSFDA (**Este no es un canal para pacientes y/o sus familiares**). Esto incluye, pero no se limita a:

1. Empleados de cualquiera de las entidades vinculadas a HUSFDA.
2. Accionistas, partícipes y personas pertenecientes al Órgano de Administración, incluidos los miembros no ejecutivos.
3. Cualquier persona que trabaje para o bajo la supervisión y dirección de contratistas, subcontratistas y proveedores.
4. Personal autónomo.
5. Voluntarios, becarios o trabajadores en formación.
6. Personal cuya relación laboral aún no haya comenzado y tengan información durante el proceso de selección o la negociación del contrato.
7. Personal cuya relación laboral ya ha finalizado.

9. ¿QUÉ CONDUCTAS PUEDEN INFORMARSE A TRAVÉS DEL CANAL?

Las conductas que son susceptibles de comunicación a través del Canal interno de información se encuadran dentro de las siguientes categorías:

1. Ilícitos penales:

- (i) Contratación Pública
- (ii) Servicios, productos y mercados financieros
- (iii) Blanqueo de Capitales o financiación del terrorismo
- (iv) Seguridad y conformidad de los productos comercializados
- (v) Seguridad del transporte
- (vi) Protección del medio ambiente
- (vii) Protección frente a radiaciones y seguridad nuclear
- (viii) Seguridad de los alimentos y los piensos, la sanidad animal y bienestar de los animales
- (ix) Salud Pública
- (x) Protección de los consumidores
- (xi) Protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información
- (xii) Intereses financieros de la Unión y mercado interior
- (xiii) Corrupción Pública o privada
- (xiv) Acoso laboral o sexual
- (xv) Propiedad industrial o intelectual
- (xvi) Libre competencia
- (xvii) Subvenciones, Hacienda Pública o Seguridad Social
- (xviii) Integridad moral o los Derechos Humanos
- (xix) Cohecho
- (xx) Tráfico de influencias
- (xxi) Conflictos de intereses
- (xxii) Prevención de riesgos laborales

2. Otras infracciones penales.

3. Otras infracciones administrativas graves o muy graves.

En el caso de tratarse de una comunicación sobre acoso sexual o por razón de sexo, se seguirá el Protocolo de acoso sexual por razón de sexo y/o de carácter discriminatorio aprobado por HOSPITAL UNIVERSITARIO SAN FRANCISCO DE ASIS(HUSFDA)el 6 de febrero de 2020, y, en caso de tratarse de acoso laboral, se seguirá el Protocolo sobre acoso laboral o mobbing aprobado por HOSPITAL UNIVERSITARIO SAN FRANCISCO DE ASIS el 6 de febrero de 2020.

10. GARANTÍAS Y MEDIDAS DE PROTECCIÓN

HUSFDA garantiza la profesionalidad, justicia e imparcialidad, así como la gestión por personal cualificado (el Responsable del Sistema). Para ello, el Sistema interno de información de se rige por los siguientes principios generales:

Anonimato del informante

El canal de comunicación establecido por HUSFDA permite la presentación de comunicaciones anónimas. Por ello el informante podrá, a su libre elección, identificarse o presentar su comunicación de manera anónima. No obstante, se anima a que, en el momento de formular su comunicación, el

informante facilite un medio de comunicación seguro y fiable para poder mantener un dialogo con el Instructor encargado de la investigación de la comunicación. Así se podrá obtener más información y resolver posibles dudas con el informante sobre los hechos comunicados.

En caso de que el informante se identifique, el Sistema garantizará su anonimato, protegiendo el derecho a que su identidad no sea revelada a terceras personas ajenas al tratamiento de la información facilitada, con la única excepción de la comunicación a la Autoridad judicial o administrativa, o al Ministerio Fiscal, en el ámbito de una investigación oficial por parte de los mismos.

Para ello, el Procedimiento de gestión cuenta con medidas técnicas y organizativas que preservan la identidad del informante y garantizan la confidencialidad de los datos tratados en las informaciones facilitadas.

Confidencialidad

El Sistema utiliza medios de comunicación eficaces que garantizan y preservan la confidencialidad tanto del informante como de la información tratada.

HUSFDA garantiza la confidencialidad del informante, así como su protección frente a posibles represalias, adoptando las medidas adecuadas para ello, entre otras, encargando la gestión del Sistema interno de información a un tercero externo.

En HUSFDA resulta esencial que el informante goce de una protección apropiada, garantizándole en todo momento la privacidad e integridad de la información facilitada, restringiéndose el acceso a la misma únicamente a aquellas personas encargadas de su gestión y tramitación. De este modo, salvo aquellas excepciones previstas legalmente, la identidad del informante no se facilitará a ningún tercero. Además, las personas de HUSFDA que, por sus funciones, puedan tener acceso y conocer las comunicaciones que se presenten y la identidad del informante, están obligadas a guardar la debida confidencialidad y secreto profesional, tanto sobre la identidad del informante como sobre su contenido.

Prohibición de represalias

HUSFDA no tolerará represalias (incluidas las amenazas y las tentativas de represalia) contra ningún informante por plantear una comunicación, o cualquier inquietud de buena fe o por cooperar en la investigación, y adoptará sus mayores esfuerzos para evitar, perseguir y sancionar tales conductas.

Se entiende por represalia cualquier acto que suponga un perjuicio o trato desfavorable por su condición de informante, como pueden ser, la suspensión del contrato de trabajo, daños de carácter reputacional o la denegación de formación, entre otros.

Los actos constitutivos de represalia serán nulos y darán lugar a medidas disciplinarias o de responsabilidad, incluyendo una indemnización de daños y perjuicios.

De igual manera, la persona afectada por la comunicación gozará del derecho de protección, preservándose su identidad, así como la confidencialidad de la información y del Procedimiento de gestión de la misma.

Esta prohibición de represalias no impedirá, cuando corresponda, la adopción de medidas disciplinarias cuando la investigación interna determine que la comunicación era falsa y que el informante era consciente de su falsedad, actuando así de mala fe. En estos casos, las comunicaciones o acusaciones que se demuestren falsas, no honestas o realizadas con la única finalidad de perjudicar a otras personas, obtener algún beneficio en el trabajo o eludir deberes laborales, se remitirán a la Dirección de Recursos Humanos en caso de empleados o se tomarán cualesquiera acciones que en Derecho pudieran corresponder.

Quedan expresamente excluidas de protección las siguientes comunicaciones:

1. Inadmitidas por el Canal interno de información.
2. Contrarias a la buena fe.
3. Vinculadas a reclamaciones sobre conflictos interpersonales entre el informante y la persona afectada por la información.
4. Disponibles para el público.

Derechos de la “persona afectada por la información”

Con respecto a la persona afectada por la información, la misma gozará, como no puede ser de otro modo, de los siguientes derechos:

- **Derecho a ser informado de la admisión a trámite de la comunicación:** en el caso de existir una persona física afectada, tiene derecho a ser informada en el **plazo de treinta (30) días** desde la fecha de recepción de la comunicación.
- **Derecho a la presunción de inocencia de la persona afectada por la información:** toda persona se presume inocente y será tratada como tal durante toda la tramitación del expediente de investigación, mientras no se demuestre su responsabilidad respecto de los hechos comunicados.
- **Derecho de defensa:** garantía de la persona afectada por la información que le permite solicitar y aportar pruebas, acceder al expediente de investigación (no suponiendo ello el acceso a la identidad del informante), así como rebatir aquéllas que se presenten en su contra.
- **Derecho de asistencia:** La persona afectada por la información tiene derecho a asistir a la entrevista con un abogado, un representante legal de los trabajadores o cualquier persona que elija.

Información, accesibilidad y formación

HUSFDA informará del presente Protocolo a través de su página web, de forma accesible e identificable, así como de la existencia del Canal de comunicación interno de información.

Además, con respecto a sus empleados, podrán acceder al Protocolo a través de la Intranet de la Organización, del mismo modo HUSFDA desarrollará actividades de formación con el fin de fomentar el uso del Canal y de resolver cuantas dudas pudieran surgir con respecto al mismo.

Evaluación

De forma anual se llevará a cabo una evaluación del funcionamiento del Canal interno de información con el fin de valorar su efectividad, así como las modificaciones o posibles mejoras que se puedan efectuar con respecto al mismo, con el objetivo de que la entidad sea la primera en conocer las posibles irregularidades que se puedan llegar a producir e impedir que su reproducción.

Procedimiento disciplinario y sancionador

HUSFDA adoptará las medidas disciplinarias que correspondan dependiendo de la infracción cuya comisión resulte acreditada, incluyendo las disciplinarias (en el ámbito laboral) o contractuales (en las relaciones mercantiles con Terceros) que considere proporcionales al riesgo o daños ocasionados.

Las medidas que se adopten desde una perspectiva laboral serán respetuosas con la normativa aplicable, sin que por ello pierdan contundencia o proporcionalidad con la gravedad de los hechos de los que traigan causa, informando si procede a la Representación Legal de los Trabajadores.

Del mismo modo, impondrá las sanciones que entienda oportunas a aquellos informantes que actúen de mala fe.

Conservación

Los datos personales facilitados relativos a las informaciones recibidas, tanto a la gestión de las mismas como a los datos del informante y de las personas afectadas, se conservarán únicamente durante el tiempo imprescindible para estudiar, investigar y resolver el caso.

En particular, los datos que sean objeto de tratamiento podrán conservarse en el canal de comunicación interno únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.

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

Si una vez transcurridos **tres meses** desde la recepción de la comunicación no se hubiesen iniciado ninguna actuación de investigación, se procederá a la supresión de los datos, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del Canal.

Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

En ningún caso se conservarán los datos en el Canal de comunicación interno por un período superior a **diez años**.

11. CONFLICTOS DE INTERESES.

Se entenderá que existe riesgo de **conflicto de interés** cuando una persona participe en la investigación de la comunicación en los siguientes supuestos:

- Existencia de **vínculo familiar** con el informante o investigado (ascendiente, descendiente, cónyuge o pareja de hecho y/o hermanos);
- Estar o haber sido informado **previamente** por el informante;
- Resultar **afectado** por los hechos comunicados y no haberlo comunicado;
- Formar **parte del área o departamento** afectado por la comunicación;
- Existencia de **amistad o enemistad manifiesta** con el informante o investigado;
- Estar o haber estado en situación de **dependencia jerárquica** respecto del informante o investigado en los últimos doce meses;

En el caso de recibir una comunicación a través del Canal dirigido contra uno o más miembros del Comité o del comité de dirección, o que pudiese afectar de manera directa o indirecta por existir un conflicto de interés, el Responsable del Sistema y el Instructor, De Lorenzo Abogados, garantizarán que no remitirán esa comunicación a las personas afectadas, y procederá directamente con la investigación de los hechos, pudiendo en todo caso contar con el asesoramiento de un experto externo o de otros departamentos de HUSFDA.

12. CANAL EXTERNO DE LA AUTORIDAD INDEPENDIENTE DE PROTECCIÓN AL INFORMANTE.

La Autoridad Independiente de Protección del Informante (AIPI) será el ente encargado de la gestión del Canal Externo de Informaciones establecido en el Título III de la referida Ley de Protección del Informante, y se constituye, así como el pilar básico del sistema institucional en materia de protección del informante.

La Autoridad Independiente de Protección del Informante además de gestionar el Canal de comunicación Externo al cual pueden acudir tanto trabajadores del sector público como del privado, será la autoridad competente para la tramitación, a través del referido Canal externo, las comunicaciones, o reportes que afecten a los siguientes sujetos:

1. La Administración General del Estado y entidades que integran el sector público estatal.
2. Las Administraciones de las comunidades autónomas, las entidades que integran la Administración y el sector público institucional autonómico o local, cuando se atribuya la competencia a la Autoridad Independiente de Protección del Informante, en virtud de un convenio.
3. Resto de entidades del sector público, los órganos constitucionales y los órganos de relevancia constitucional a que se refiere el artículo 13.
4. Entidades que integran el sector privado, cuando la infracción o el incumplimiento informado afecte o produzca sus efectos en el ámbito territorial de más de una comunidad autónoma.

En este sentido, debemos manifestar que el canal externo dependiente de la Autoridad independiente del de Protección al Informante es autónomo del Canal interno de información implantado en HUSFDA, en consecuencia, el informante tendrá la opción de utilizar el Canal que estime oportuno.

En conclusión, cualquier informante podrá comunicar ante dicha Autoridad, o ante las autoridades u órganos autonómicos correspondientes, de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación de la citada ley. **(LA INFORMACIÓN DE ACCESO AL CANAL EXTERNO AÚN NO PUBLICADA POR EL MINISTERIO DE JUSTICIA)**

13. DIFUSIÓN Y ENTRADA EN VIGOR.

El presente Protocolo entrará en vigor de forma general para HUSFDA, el 13 de junio de 2023.

El Protocolo se entrega y está a disposición de todos los miembros de HUSFDA mediante su publicación en la [intranet].

Igualmente, HUSFDA, pondrá a disposición de terceros el Protocolo a través de la página web donde se encuentre habilitado el Canal de comunicación interno de información.

HUSFDA comunicará por las mismas vías cualquier modificación sobre el presente Protocolo.