



# SISTEMA INTERNO DE INFORMACIÓN

---

# PROTOCOLO



## REGISTRO DE ACTUALIZACIONES DEL DOCUMENTO

<b>Versión</b>	<b>Fecha actualización</b>	<b>Apartado(s) objeto de actualización</b>	<b>Observaciones</b>
V.00	01/12/2023	Versión inicial	Documento inicial

## Contenido

REGISTRO DE ACTUALIZACIONES DEL DOCUMENTO .....	2
1. OBJETO .....	4
2. NORMATIVA Y LEGISLACIÓN DE REFERENCIA .....	4
3. ÁMBITO DE APLICACIÓN .....	5
3.1. Ámbito objetivo .....	5
3.2. Ámbito subjetivo .....	5
4. PRINCIPIOS RECTORES.....	6
5. PRINCIPALES ACTORES Y RESPONSABLES EN EL SISTEMA INTERNO DE INFORMACIÓN .....	8
6. MEDIOS HABILITADOS PARA INFORMAR .....	9
7. CONTENIDO DE LA COMUNICACIÓN.....	10
8. PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES .....	11
9. MEDIDAS DE PROTECCIÓN DEL INFORMANTE.....	14
10. MEDIDAS DE PROTECCIÓN DE LAS PERSONAS AFECTADAS.....	15
11. CANAL EXTERNO .....	16
12. INCUMPLIMIENTO.....	16
13. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.....	16
14. PUBLICACIÓN Y DIFUSIÓN DEL SISTEMA INTERNO DE INFORMACIÓN ...	18
15. REVISIÓN DEL PROTOCOLO DEL SISTEMA INTERNO DE INFORMACIÓN	18
16. ENTRADA EN VIGOR.....	18

## 1. OBJETO

El presente documento de protocolo tiene como objetivo establecer el Sistema Interno de Información, gestión, investigación y respuesta de la Diócesis de Astorga (en adelante, también la Entidad), a través del cual, garantizando la protección del informante, se pueden comunicar todos los actos de los que se tenga conocimiento, que puedan ser susceptibles de ilícitos penales y/o de infracciones administrativas graves o muy graves.

El protocolo o procedimiento que en este documento se recoge:

- (i) delimita el alcance del Sistema interno de información,
- (ii) proporciona las pautas de actuación una vez recibida la comunicación,
- (iii) identifica las responsabilidades de cada uno de los intervinientes y
- (iv) define los principios y garantías que priman en el sistema.

## 2. NORMATIVA Y LEGISLACIÓN DE REFERENCIA

El Sistema interno de información de la Diócesis de Astorga se ha configurado en virtud de los requerimientos técnicos y legales previstos en la siguiente normativa:

- Directiva 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 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

## 3. ÁMBITO DE APLICACIÓN

### 3.1. Ámbito objetivo

#### ¿Qué puede comunicarse?

A través del Sistema interno de información contemplado en este protocolo podrá remitirse información relativa a:

- Acciones u omisiones que puedan ser **constitutivas de infracción penal o administrativa grave o muy grave.**
- Especialmente, acciones u omisiones que puedan ser **constitutivas de infracciones del Derecho laboral en materia de seguridad y salud en el trabajo.**
- Cualesquiera acciones u omisiones que puedan **constituir infracciones del Derecho de la Unión Europea**, siempre que (i) estén incluidas en el ámbito material de aplicación de los actos de la Unión Europea enumerados en el anexo de la Directiva 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, (ii) afecten a los intereses financieros de la Unión Europea o (iii) incidan en el mercado interior.

### 3.2. Ámbito subjetivo

#### ¿Quién puede comunicarlo?

Este protocolo del Sistema interno de información resultará de aplicación a cualquier informante que haya obtenido información sobre infracciones en un contexto laboral o profesional, siempre que se trate de:

- Trabajadores por cuenta ajena.
- Autónomos.
- Personas pertenecientes al órgano de administración, dirección o supervisión de la Diócesis, incluidos los miembros no ejecutivos.

- Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.
- Voluntarios, becarios y otros referidos en la Ley 2/2023.

## 4. PRINCIPIOS RECTORES

A continuación, se detallan los principios y compromisos de la Diócesis de Astorga respecto del Sistema interno de información:

### **SISTEMA DE COMUNICACIÓN**

Establecer un Sistema interno de información que permita la recepción y gestión de comunicaciones escritas o verbales, contribuyendo con ello a una adecuada comunicación sobre posibles irregularidades o ilícitos indicados.

### **SEGURIDAD**

Diseñar, establecer y gestionar el Sistema interno de información de 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 la misma, además de la protección de datos, impidiendo el acceso de personal no autorizado.

### **SIGILO**

El Sistema implantado vela por que las personas implicadas en la tramitación e investigación de las comunicaciones actúen con la máxima discreción sobre los hechos que conozcan por razón de su cargo o función.

### **BUENA FE**

Toda información facilitada debe atender a criterios de veracidad y buena fe, evitando proporcionar información confusa, falsa o carente de toda fidelidad. Cualquier incumplimiento de lo dispuesto en el presente protocolo puede conllevar la aplicación de medidas sancionadoras.

<b>EFFECTIVIDAD</b>	Garantizar que las comunicaciones presentadas puedan tratarse de forma efectiva dentro de la Entidad, de manera que la primera en conocer la posible irregularidad sea la propia Diócesis.
<b>TRANSPARENCIA</b>	Generar un entorno de transparencia y eficiencia en todo el procedimiento de gestión. La información será proporcionada de forma clara y fácilmente accesible, y con publicidad suficiente sobre su uso y principios y garantías rectores.
<b>PROTECCIÓN</b>	Garantizar la protección del informante, de quienes le asistan, de sus compañeros o familiares y de las personas jurídicas para las que trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa.
<b>TOLERANCIA CERO</b>	Promover una cultura de “tolerancia cero” hacia la comisión de irregularidades, así como hacia la adopción de medidas de represalia con motivo del uso del Sistema.
<b>APOYO</b>	Ofrecer las medidas de apoyo y/o protección necesarias al informante.
<b>DERECHOS</b>	Asegurar y respetar la presunción de inocencia, el honor y el derecho de defensa de la persona afectada durante todo el proceso.
<b>COLABORACIÓN CON LAS AUTORIDADES</b>	Colaborar con las autoridades administrativas de control, Ministerio Fiscal, Fuerzas y Cuerpos de Seguridad del Estado u otras administraciones autonómicas o locales competentes, incluso de la Unión Europea, en los procesos de investigación que requirieran su intervención.

<b>PROTECCIÓN DE DATOS</b>	Adoptar las medidas correspondientes en materia de protección de datos.
<b>CONTROL</b>	Garantizar un seguimiento y control del Sistema, a fin de adaptarlo a las circunstancias concurrentes y exigibles en cada momento.
<b>ANONIMATO</b>	Cuando así se requiera por el informante.

## 5. PRINCIPALES ACTORES Y RESPONSABLES EN EL SISTEMA INTERNO DE INFORMACIÓN

- **Responsable del Sistema Interno de Información:** el Obispo de la Diócesis ha designado a una persona como Responsable del Sistema, que actuará con autonomía e independencia. Su nombramiento será notificado a la Autoridad Independiente de Protección al Informante, A.A.I. estatal, o, en su caso, a las autoridades u órganos competentes de la Comunidad Autónoma de Castilla y León, en el plazo de los diez días hábiles siguientes.

Responderá de la tramitación diligente del procedimiento de gestión de informaciones, para lo cual:

- Controlará el Sistema interno de información.
- Recibirá la valoración inicial remitida por el equipo legal externo.
- Llevará el libro – registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar, garantizando, en todo caso, la confidencialidad. Solo a petición razonada de la Autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquélla, podrá accederse total o parcialmente al contenido del referido registro. Los datos personales relativos a las informaciones recibidas y a las



investigaciones internas solo se conservarán durante el período estrictamente necesario y proporcionado a efectos de cumplir con los trámites previstos legalmente.

- Custodiará toda la documentación presentada a través del Sistema interno de información.
- Realizará la función instructora, consistente en:
  - Archivo o admisión a trámite de la comunicación.
  - Si procediera, iniciar fase de investigación.
  - Elaborar informe de conclusiones y resolución, con las medidas propuestas.
  - Garantizar la protección del informante y de la persona afectada.
  
- **Equipo legal externo:** despacho de abogados externo a la Entidad que colaborará con el Responsable del Sistema y asesorará en la primera valoración y la posterior gestión del Sistema interno de información. Este equipo ofrece las garantías adecuadas de respeto de la independencia, confidencialidad, protección de datos y secreto de las comunicaciones.
  
- **Informante:** persona que, siempre con veracidad y buena fe, informa o comunica cualquiera de los riesgos o incumplimientos contenidos en el ámbito objetivo.
  
- **Persona afectada:** aquella a la que se le atribuye la comisión de un incumplimiento y goza de la presunción de inocencia.

## 6. MEDIOS HABILITADOS PARA INFORMAR

Las comunicaciones que contengan información sobre las posibles infracciones o a las que se hace mención en el ámbito

objetivo del presente protocolo, deberán realizarse a través de alguna de las siguientes vías:

- Enlace situado en la página web:  
[www.diocesisastorga.es](http://www.diocesisastorga.es)
- Código QR, que se obtiene en la misma página web.
- Correo postal dirigido al Responsable del Sistema:  
    Diócesis de Astorga (ATT. Responsable SII)  
    C/ Carmen, 2  
    24700 de Astorga (León)
- Reunión presencial con el Responsable del Sistema, que se documentará, bien mediante una grabación de la conversación en un formato duradero y accesible, bien a través de un acta pormenorizada de la reunión.

Cualquier otra forma de comunicación se redirigirá, si fuera necesario, al Responsable del Sistema y se transcribirá a un medio escrito y fiable.

## 7. CONTENIDO DE LA COMUNICACIÓN

La comunicación realizada mediante el Sistema interno de información, sin perjuicio de las garantías recogidas en la normativa vigente, deberá encaminarse hacia la eficacia del proceso a efectos de evitar indefensión e inseguridad jurídica de las partes implicadas.

En este sentido, deberá contener **información suficiente** que permita su delimitación y verificación en los distintos planos de la comunicación, tales como:

- **Identificación del supuesto agresor** o de los **implicados**, en la medida de lo posible, nombre y apellidos o, en su defecto, puesto que ocupa, turno en el que ha trabajado, siempre que pueda ofrecerse tal información y siempre que exista esta figura.

- **Identificación de la supuesta víctima**, nuevamente, ofreciendo información suficiente que no paralice el proceso.
- **Identificación del denunciante y de los posibles testigos** que hayan presenciado los hechos, así como de los posibles **afectados** o **implicados**.
- **Lugar** en el que han ocurrido los hechos, especificando con la mayor concreción posible la dirección, el centro de trabajo, espacio, lugar, etc.
- Hora, momento, turno o acotación del **ámbito temporal** en el que supuestamente ha tenido lugar el acontecimiento.
- **Hechos o supuesta infracción, sospechas, indicios** que constan al denunciante con el máximo detalle posible. Es de interés recordar que, en la medida de lo posible, la máxima amplitud de esta información garantiza evitar la pérdida de información o datos que pueda darse a medida que pase el tiempo y los detalles puedan caer en el olvido.
- Información que pueda agregar valor a la comunicación.

## 8. PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES

Recibida la comunicación por el Responsable del Sistema, éste enviará el acuse de recibo al informante en el plazo de siete días naturales siguientes a su recepción (salvo que ello pueda poner en peligro la confidencialidad de la comunicación).

En el supuesto de recibir una comunicación persona ajena al Responsable del Sistema, el receptor deberá trasladarla a éste, respetando, en todo caso, los deberes de confidencialidad y, si así se hubiera solicitado, de preservación del anonimato del informante. El quebranto de estos principios puede suponer la comisión de una infracción muy grave.

Cualquiera que fuere el medio, recibida la información por el Responsable del Sistema interno, deberá decidir si esa información es **admitida o no a trámite**, para lo que se servirá de la colaboración para la valoración no vinculante del equipo legal externo. Serán inadmitidas las siguientes comunicaciones:

- Que carezcan de indicios suficientes de verosimilitud.
- Que los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico incluida en el ámbito de aplicación objetivo.
- Que carezcan manifiestamente de fundamento o existan indicios racionales de haberse obtenido mediante la comisión de un delito.
- Que no contengan información nueva y significativa sobre infracciones, en comparación con una comunicación anterior respecto de la cual han concluido los correspondientes procedimientos.
- Que no se refieran a hechos o datos concretos que permitan su esclarecimiento o se basen en rumores o en opiniones o informaciones poco fundamentadas.

Es obligación del informante hacer un uso responsable de este Sistema interno de información, por lo que en ningún caso ha de realizar denuncias infundadas o de mala fe, pudiendo derivarse en tal caso las acciones legales y/o de carácter disciplinario que resulten de aplicación. Además, corresponde al informante garantizar que los datos proporcionados son veraces, exactos y lo más completos posible.

El Responsable del Sistema podrá requerir al informante para que aporte información adicional, no pudiendo exigírsele su identificación.

Cuando los hechos pudieran ser indiciariamente constitutivos de delito, se remitirá la información con carácter inmediato al Ministerio Fiscal. Y si los hechos afectaran a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

La admisión a trámite de la información implicará la apertura de un expediente, al que se asignará un código de identificación. Si existieran trámites de informaciones sobre los mismos hechos, se acumularán en un único expediente. Con ello se inicia la fase de investigación, dirigida por el Responsable del Sistema.

Durante esta fase de investigación, se informará a la persona afectada de las acciones u omisiones que se le atribuyen, dándole trámite para que, en el plazo que se considere oportuno, formule las alegaciones que estime pertinentes, con la finalidad de permitirle ejercer su derecho de defensa.

Asimismo, todo el personal deberá cooperar con el Responsable del Sistema en aquello que se le pudiera requerir.

Concluida la fase de investigación, el Responsable emitirá la correspondiente resolución. Dicha resolución podrá suponer:

- El archivo de las actuaciones: si no hubiera evidencias suficientes o si, tras las averiguaciones oportunas, no se hubiera podido concluir la comisión de ninguna infracción.
- La adopción de medidas preventivas, detectivas o reactivas: si se concluye que se ha cometido una irregularidad o infracción.
  - Medidas preventivas: aquellas tendentes a evitar que el incumplimiento se vuelva a repetir o que minimicen su impacto o probabilidad de su ocurrencia en el futuro. Por ejemplo, la adopción o modificación de políticas corporativas, normas internas, cambios organizativos, procesos o procedimientos, programas o planes, acciones formativas, de comunicación o sensibilización, entre otras.
  - Medidas detectivas: aquellas tendentes a permitir o facilitar que en el futuro se puedan descubrir o detectar, con anterioridad a que se produzcan o

en una fase muy temprana tras su producción, posibles incumplimientos. Constituyen medidas detectivas, por ejemplo, la realización de actividades de monitorización, la implantación de sistemas reforzados de autorizaciones o el establecimiento de indicadores de riesgo y su medición periódica.

- Medidas reactivas: aquellas que se adoptan para evitar que los incumplimientos queden sin respuesta punitiva o resarcitoria desde el punto de vista disciplinario, contractual y/o de la legalidad vigente.

La resolución se comunicará tanto al informante, salvo que éste fuere anónimo, como a la persona afectada.

El **plazo máximo para dar respuesta a las actuaciones de investigación**, mediante la consiguiente resolución, no podrá ser superior a tres meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante, a tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, éste podrá extenderse hasta un máximo de otros tres meses adicionales.

## 9. MEDIDAS DE PROTECCIÓN DEL INFORMANTE

La Diócesis de Astorga prohíbe expresamente los actos constitutivos de represalia, incluidas las amenazas y tentativas de represalia, contra las personas que, de buena fe, presenten una comunicación a través del Sistema interno de información.

A estos efectos, se entiende por represalia la adopción de cualquier medida que implique un trato de coacción, hostilidad, discordia o aversión contra el informante, entre las que se incluyen:

- Suspensión, despido, destitución o medidas equivalentes, cuyo origen radique en la comunicación de denuncia.
- Modificaciones perjudiciales de las funciones y responsabilidades laborales, cambio de centro de trabajo, reducción salarial, etc.
- Denegación de ascensos.
- Denegación de formación.
- Tratos discriminatorios, vejatorios, denigrantes o humillantes.
- Evaluación o referencias negativas.
- Denegación de permisos.

A fin de evitar la imposición de represalias y asegurar la protección del informante, la Entidad podrá adoptar las medidas que estime convenientes para cada caso. A modo de ejemplo, dichas medidas podrán consistir en (i) velar por la confidencialidad de los hechos y datos aportados, además de por el anonimato del informante, o (ii) realizar un seguimiento periódico de sus condiciones profesionales tras la finalización de la investigación. Todo ello sin perjuicio de que pueda valorarse la posibilidad de realizar, coyunturalmente, un cambio de área, departamento o puesto de trabajo.

## **10. MEDIDAS DE PROTECCIÓN DE LAS PERSONAS AFECTADAS**

Durante el procedimiento de gestión de la comunicación, se garantizará el derecho a la presunción de inocencia, el derecho de defensa y el derecho de acceso al expediente de las personas afectadas, así como a la misma protección establecida para los informantes, preservándose su identidad y la confidencialidad de los hechos y datos del procedimiento.

## **11. CANAL EXTERNO**

Toda persona física podrá informar, sea directamente, sea previa comunicación a través del Sistema interno de información, a la Autoridad Independiente de Protección del Informante, A.A.I., o a las autoridades u órganos autonómicos correspondientes, de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito objetivo de aplicación de la Ley 2/2023.

## **12. INCUMPLIMIENTO**

Todo incumplimiento del presente protocolo del Sistema interno de información o uso inadecuado del mismo podrá ser constitutivo de infracción y, en consecuencia, susceptible de la aplicación de las correspondientes medidas disciplinarias.

## **13. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

Los datos que se proporcionen a través del Sistema interno de información serán tratados por la Diócesis de Astorga para la gestión de la comunicación recibida en el Sistema, así como para la realización de cuantas investigaciones sean necesarias para determinar la comisión de la supuesta infracción. El acceso a la información se ajustará a lo establecido en este procedimiento y a la legislación vigente en materia de protección de datos.

La Diócesis de Astorga se compromete a tratar, en todo momento, los datos de carácter personal recibidos a través del Sistema interno de información de forma absolutamente confidencial y de acuerdo con las finalidades previstas en este procedimiento, adoptando las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los



datos almacenados y los riesgos a los que están expuestos, en cumplimiento de lo dispuesto en la legislación sobre protección de datos de carácter personal.

En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la ley.

Si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de estos.

También será suprimida la información que no sea veraz, procediéndose a la supresión desde el momento en que se tenga constancia, salvo que la falta de veracidad constituya un ilícito penal. En ese caso, se guardará la información durante el tiempo necesario para la tramitación del procedimiento judicial.

No se revelará la identidad del informante sin su consentimiento expreso a ninguna persona que no sea un miembro autorizado del personal competente para recibir o seguir informaciones. Lo anterior también se aplicará a cualquier otra información de la que se pueda deducir directa o indirectamente la identidad del informante.

Como excepción al apartado anterior, la identidad del informante solo podrá revelarse cuando constituya una obligación necesaria y proporcionada impuesta por las leyes vigentes, en el contexto de una investigación llevada a cabo por las autoridades nacionales o en el marco de un proceso judicial, en particular para salvaguardar el derecho de defensa de la persona afectada. Se avisará al informante antes de revelar su identidad, salvo que dicha

revelación pudiera comprometer la investigación o el procedimiento judicial.

Las personas que efectúen una comunicación a través del Sistema interno de información deberán garantizar que los datos personales proporcionados son verdaderos, exactos, completos y actualizados.

## **14. PUBLICACIÓN Y DIFUSIÓN DEL SISTEMA INTERNO DE INFORMACIÓN**

Este protocolo del Sistema interno de información de la Diócesis de Astorga será objeto de publicación y difusión a través de la página web de la Entidad y de aquellas otras de las que pudieran disponer los distintos centros de trabajo.

## **15. REVISIÓN DEL PROTOCOLO DEL SISTEMA INTERNO DE INFORMACIÓN**

Tanto este protocolo como el procedimiento de gestión de las comunicaciones estarán sometidos a las evaluaciones y revisiones periódicas correspondientes, a los efectos de detectar aspectos de mejora y acomodarse a las indicaciones, pautas o recomendaciones que puedan trasladarse.

Las posibles modificaciones del presente protocolo serán aprobadas por el Obispo de la Diócesis.

## **16. ENTRADA EN VIGOR**

El presente protocolo del Sistema interno de información ha sido aprobado por el Obispo de la Diócesis de Astorga y entrará en vigor a partir de esta fecha.

En Astorga, a 1 de diciembre de 2023.



