PGCP- 06. Procedimiento Sistema Interno de Información (Canal de Denuncias)

Ed. 01 · 01/01/2023

I. OBJETO

El Sistema Interno de Información se establece no sólo para dar cumplimiento a un requisito legal impuesto por la Directiva 2019/1937 de 23 de octubre y su transposición 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, sino para posibilitar que los empleados y terceros puedan comunicar a la organización, las infracciones señaladas en el artículo 2 de la Ley y puedan ser protegidas frente a cualquier tipo de represalia.

II. ALCANCE

Concretamente en este procedimiento se abordan los siguientes aspectos:

- Qué acciones procede planificar para que el Sistema Interno de Información cumpla con la Ley 2/2023 a efectos de prevenir, detectar y gestionar los riesgos penales.
- Cómo realizar las comunicaciones y cómo proteger a los informantes respetando los derechos de las personas afectadas.
- Cómo establecer objetivos concretos y medibles que ayuden a constatar la evolución del sistema y puedan adoptarse las mejores decisiones justo a tiempo.

III. DEFINICIONES

1. **Infracciones:** las acciones u omisiones que sean ilícitas y estén relacionadas con las siguientes materias:
    a. Contratación pública.
    b. Servicios, productos y mercados financieros y prevención del blanqueo de capitales y la financiación del terrorismo.
    c. Seguridad de los productos y conformidad.
    d. Seguridad del transporte.
    e. Protección del medio ambiente.
    f. Protección frente a las radiaciones y seguridad nuclear.
    g. Seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales.
    h. Salud pública.
    i. Protección de los consumidores.
    j. Protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información.
    k. Infracciones que incidan en el mercado interior europeo (competencia, ayudas de los Estados, ventajas fiscales o infracciones sobre el impuesto de sociedades).
    l. Acciones u omisiones que puedan constituir infracciones penales o administrativas graves o muy graves, incluyendo siempre las que afecten a un quebranto económico a la Hacienda Pública y a la Seguridad Social.
    m. Infracciones o incumplimientos de nuestro Código Ético y del Sistema de Gestión de Compliance Penal, sus Políticas y procedimientos.

2. **Información sobre infracciones:** la información, incluidas las sospechas razonables, sobre infracciones reales o potenciales, que se hayan producido o se vayan a producir en la organización en la que trabaje o haya trabajado el informante o en otra organización que por motivo de trabajo haya estado en contacto el informante; y sobre intentos de ocultar tales infracciones.
3. **Sistema interno de información:** cauce preferente para informar sobre las acciones previstas en el artículo 2 de la Ley 2/2023.
4. **Gestión del Sistema de recepción:** la recepción de informaciones.
5. **Canal interno de información:** todo aquel que permita a una entidad presentarle información sobre infracciones previstas en el artículo 2 de la Ley 2/2023.
6. **Responsable del Sistema Interno de Información:** persona designada por el órgano de gobierno que desarrolla las funciones de tramitación diligente del procedimiento de gestión de informaciones de forma independiente y autónoma.
7. **Canal externo:** la comunicación verbal o por escrito de información sobre infracciones ante las autoridades competentes.
8. **Revelación pública o revelar públicamente**: la puesta a disposición del público información sobre infracciones.
9. **Informante:** persona física que comunica o revela públicamente información sobre infracciones obtenida en el contexto de sus actividades laborales.
10. **Facilitador:** persona física que asiste a un informante en el proceso de comunicación en un contexto laboral y cuya asistencia debe ser confidencial.
11. **Contexto laboral:** las actividades de trabajo presentes o pasadas en el sector público o privado a través de las cuales, las personas pueden obtener información sobre infracciones y en el que estas personas podrían sufrir represalias si comunicarán dicha información.
12. **Persona afectada:** persona física o jurídica a la que se haga referencia en la comunicación o revelación pública como la persona a la que se atribuye la infracción o con la que se asocia la infracción.
13. **Represalia:** toda acción u omisión, directa o indirecta, que tenga lugar en un contexto laboral, que esté motivada por una comunicación o revelación pública y que cause o pueda causar perjuicios injustificados al informante.
14. **Seguimiento:** toda acción emprendida por el destinatario de una comunicación o autoridad competente a fin de valorar la exactitud de las alegaciones hechas en la comunicación, y en su caso,

resolver la infracción comunicada, incluso a través de investigaciones internas, acciones judiciales, acciones de recuperación de fondos o el archivo del procedimiento.

15. **Respuesta:** la información facilitada a los informantes sobre las medidas previstas o adoptadas para seguir la comunicación y los motivos de tal seguimiento.

16. **Autoridad competente:** toda autoridad nacional designada para recibir comunicaciones y dar respuesta a los informantes, y hacer el seguimiento.

IV. DOCUMENTACIÓN DE REFERENCIA/NORMATIVA

- 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 2019/1937 de 23 de octubre.
- Código Penal.

V. POLÍTICA DEL SISTEMA INTERNO DE INFORMACIÓN (CANAL DE DENUNCIAS)

El órgano de gobierno de GRUPO AVANZA en el desarrollo de su compromiso con el Código Ético como norma de máximo nivel y el cumplimiento de la legalidad, encargará al Compliance Officer la elaboración de una Política específica para el desarrollo, implementación y gestión del Canal de denuncias de la empresa dando cumplimiento así a la exigencia de la Ley 2/2023 de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción en su artículo 5.2.h).

Los objetivos que determinarán los contenidos de esta política serán:

Designar a una persona responsable: Esta persona será el Compliance Officer de Grupo AVANZA.

Establecer un procedimiento claro: Se ha de detallar cómo los empleados pueden presentar sus denuncias, quién las recibirá, cómo se investigarán y cómo se tomarán medidas.

Informar a los empleados: Se deberá dejar claro el deber de informar a todos los empleados de la existencia del canal de denuncias, cómo pueden usarlo y que se garantiza la confidencialidad y fomentar su uso.

Establecer un medio seguro para las denuncias: Se establecerá un medio seguro y confidencial para que los empleados presenten sus denuncias.

Investigar y tomar medidas: Se investigarán todas las denuncias presentadas y se tomarán medidas si es necesario, incluyendo medidas disciplinarias contra los infractores. Se mantendrá informado al denunciante del progreso de la investigación y de cualquier acción tomada.

Evaluar y mejorar: Se determinará la forma de evaluar regularmente el funcionamiento del canal de denuncias y hacer mejoras según sea necesario. Esto puede incluir encuestas de satisfacción de los empleados y análisis de datos de denuncias para identificar patrones o áreas problemáticas.

Proteger jurídicamente a aquellas personas que se prestan a comunicar los incumplimientos: Evitar que, como consecuencia de ello pudieran ser represaliadas de muy diversas formas, como por ejemplo el despido, el cambio de puesto de trabajo, la pérdida de contrato en caso de ser un proveedor, etc.

El contenido mínimo de dicha Política será:

1. Objetivos.
2. Ámbito de aplicación.
3. Fundamentos de la Política.
4. Responsable del sistema interno de información.
5. Derechos de los informantes y personas afectadas.
6. Protección de datos personales.
7. Tratamiento y gestión de los incumplimientos.
8. Formación y difusión.
9. Aprobación, entrada en vigor y revisión.

Esta política será revisada anualmente por el Compliance Officer de la compañía y deberá formar parte de la capacitación en Compliance penal de toda la organización y deberá estar disponible en como información documentada catalogándose como **"Política del Sistema Interno de información (canal de denuncias)".**

VI. PROCEDIMIENTO DEL SISTEMA INTERNO DE INFORMACIÓN

Nuestro Sistema Interno de Información es seguro, garantizando la confidencialidad del informante y de cualquier tercero que se mencione en el mismo, impidiéndole el acceso a personal no autorizado.

El "Sistema Interno de Información" será gestionado por el Compliance Officer o Delegado de Cumplimiento Normativo, de forma que todas las comunicaciones se canalizarán para que de una u otra forma le lleguen a él.

El informante podrá realizar la comunicación o denuncia por los siguientes medios indistintamente:

a. A través de la web donde figura una sección separada en la página de inicio (https://www.avanzasi.es/inicio) en la que podrás acceder a nuestro sistema electrónico en el enlace **Comunicación de incumplimientos** donde tiene un formulario e información sobre el canal y la protección de datos.

b. Por escrito, mediante correo postal dirigido al Departamento de Compliance Penal de la organización con domicilio en Edificio Avanza, PCT Geolit, Av. de la Innovación, 23620 Mengíbar, Jaén.
c. A petición del informante, podrá realizar la comunicación verbalmente mediante una reunión presencial ante el Compliance Officer, en un plazo de siete días desde que se lo solicite, procediendo a ser grabada o levantando acta de la misma e informándole de sus derechos sobre protección de datos.

El informante podrá indicar un domicilio, correo electrónico o lugar seguro a efecto de recibir notificaciones.

También se permite informar de forma anónima, bien mediante correo postal sin dar información del remitente o bien mediante el acceso web en su registro anónimo, que facilita un código en el que el informante puede conocer la tramitación del expediente.

Para comunicar una denuncia, se utilizará el FOR-01-PGCP-06 "Formulario de comunicación de denuncia" que se encuentra a disposición de cualquier interesado tanto como anexo a la Política del Sistema Interno de información como en nuestra página web por si fuera de su interés.

La comunicación deberá contener como mínimo los siguientes datos:

- Identidad del informante.
- Centro de trabajo al que pertenece.
- Descripción de los hechos comunicados o denunciados.
- Correo electrónico, domicilio o lugar seguro a efecto de recibir notificaciones.
- Persona o personas involucradas con los hechos comunicados o denunciados si se conocen.
- Si actualmente los hechos siguen produciéndose.
- Documentos o pruebas (ej. Testigos que acrediten los hechos comunicados o denunciados).

Una vez producida la comunicación por cualquiera de los medios anteriormente expuestos se procederá a entregar un acuse de recibo al informante en un plazo de siete días a partir del día de recepción de la comunicación. Para dicho acuse se utilizará el FOR02-PGCP-06 "Derechos del denunciante en materia de protección de datos". En el supuesto caso de que la denuncia contuviera hechos delictivos de gravedad, el responsable del Canal de Denuncias lo pondrá en conocimiento del Responsable Jurídico para que lo remita a Fiscalía o los Juzgados si lo considera conveniente.

El Compliance Officer será la persona imparcial competente para seguir diligentemente las comunicaciones, manteniendo contacto con el informante, pudiendo pedirle información adicional si fuera necesario, estando obligado el informante a colaborar en la investigación.

El Compliance Officer podrá ayudarse de personal del departamento afectado si lo creyera necesario para realizar una correcta investigación de la comunicación, debiendo guardar absoluta confidencialidad de todo lo actuado.

El plazo para dar respuesta a la comunicación planteada no podrá ser superior a TRES MESES a partir del acuse de recibo al informante, y si no se remitió el acuse de recibo, a tres meses a partir del vencimiento del plazo de siete días después de hacer la comunicación.

En el supuesto caso de que la comunicación no fuera respondida en el tiempo anteriormente citado, el informante podrá realizar comunicación externa ante las autoridades competentes.

Recibida la comunicación por el Compliance Officer a través de los diversos cauces, examinará la misma y podrá solicitar más pruebas para su comprobación que una vez terminada dará como resultado:

a) El archivo de la comunicación por inexistencia de las infracciones o incumplimientos comunicados o por falta de pruebas con un informe de terminación.
b) En el caso de que la comunicación supusiera la adopción de medidas legales se dará cuenta inmediata al responsable de los servicios jurídicos.
c) La continuación de su tramitación, pudiendo valerse de personal de otros departamentos, y elaborando un informe de conclusiones cuyo contenido será:
    1. Identificación de las personas implicadas
    2. Descripción de los hechos
    3. Pruebas y acreditación de los mismos
    4. Comunicación a la persona afectada para que ejercite su derecho de defensa y contradicción y a ser oída en cualquier momento
    5. Conclusiones
d) El informe de conclusiones puede tener dos terminaciones:
    1. Falta de pruebas, dando lugar a la terminación del expediente y comunicando al informante y persona afectada del archivo.
    2. Confirmación de los hechos comunicados, en cuyo caso se dará traslado al responsable de Recursos Humanos para que procedan a imponer las medidas correctivas y sancionadoras que estimen convenientes conforme al sistema disciplinario de la organización.

VII. PROTECCIÓN DE DATOS

De conformidad con la Directiva 2019/1937 y la Ley 2/2023 la organización establece un registro de todas las comunicaciones recibidas, las cuales deberán ser conservadas durante el periodo que sea necesario y proporcionado, pero nunca superior a los diez años. Para ello se utilizará el FOR03-PGCP-06 "Libro Registro de Informaciones recibidas" y cuyos registros serán gestionados a través de la Plataforma Digital NormaPro limitando el acceso exclusivamente a las siguientes personas en función de los siguientes roles y permisos establecidos:

- El responsable del Sistema y a quien lo gestione (Compliance Officer);
- El responsable de RRHH u órgano competente para imponer sanciones disciplinarias;

- El responsable de los Servicios Jurídicos si procediera adoptar medidas legales;
- Los encargados de tratamiento que eventualmente se designen
- El Delegado de Protección de Datos.

Se consideran lícitos los tratamientos de datos personales necesarios para la aplicación de la Ley 2/2023.

Una vez transcurridos los tres meses desde la iniciación de la comunicación, deberá procederse a su supresión del sistema, con la excepción que permite conservarlos para dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la organización. Transcurrido ese plazo, los datos podrán seguir siendo tratados por el órgano al que corresponda la investigación de los hechos comunicados, pero no podrán conservarse en el propio sistema de información de comunicaciones.

Aquellas comunicaciones a las que no se les haya dado curso, solamente podrán constar de forma anonimizada.

Los titulares de los datos personales deben ser informados tanto de la existencia del Sistema Interno de Información, como del tratamiento de sus datos personales en relación con cualquier comunicación en la que se vean involucrados.

Dicha información se facilita en dos fases:

- Primera fase: donde se debe informar sobre la implantación del Sistema Interno de Información, la finalidad del tratamiento de datos relacionado con este sistema de información.
- Segunda fase: en el momento en el que se recibe la comunicación, se deberá informar de ello a cada uno de los afectados: informante, persona afectada, testigos, terceros afectados, etc. El responsable deberá informar al informante desde el mismo momento en el que se contacte con él sobre los siguientes datos (artículo 13 RGPD):

    - ✓ Identidad y contacto del responsable.
    - ✓ Datos del DPD en su caso.
    - ✓ Los fines del tratamiento y la base jurídica (el 6.1.c).
    - ✓ Los destinatarios de los datos personales en su caso.
    - ✓ Si hay transferencias internacionales.
    - ✓ El plazo de conservación.
    - ✓ Los derechos de ARCOPOL.
    - ✓ El derecho a reclamar ante una autoridad de control.

Con respecto al afectado por la denuncia, existirá obligación de informarle conforme al artículo 14 RGPD:

- ✓ Identidad y datos de contacto del responsable.
- ✓ Datos del DPD en su caso.
- ✓ Fines del tratamiento y base jurídica del tratamiento.
- ✓ Las categorías de datos personales de que se trate.

- ✓ Los destinatarios de los datos en su caso.
- ✓ Transferencias internacionales en su caso.

El departamento de Protección de Datos y de Compliance implantará las medidas técnicas y organizativas suficientes para preservar la confidencialidad de los datos tratados en este fichero de comunicaciones.

A la persona a la que se refieran los hechos relatados no se le informará en ningún caso de la identidad del informante.

Si la persona afectada ejerciera su derecho de oposición se presumirá que existen motivos legítimos que legitiman el tratamiento de sus datos personales salvo prueba en contrario.

VIII. OBJETIVOS DEL SISTEMA INTERNO DE INFORMACIÓN

El objetivo del "Sistema Interno de Información" es el de conseguir que todas aquellas personas que tengan conocimiento de algún incumplimiento tengan un procedimiento adecuado para ello y que protejan a los informantes contra cualquier represalia que pretenda evitar denunciar. En último término, conseguir una cultura de la información.

El "Sistema Interno de Información" contará con un Libro-Registro de las informaciones recibidas y de las investigaciones internas que se hayan producido, garantizando la confidencialidad. Para ello se utilizará el FOR03-PGCP-06 denominado "Libro Registro de Informaciones recibidas".

En el Ev06-PGCP.07 "Informe anual de Compliance para revisión por la Dirección" se incluirá un anexo que será catalogado como Ev03-PGCP-06 "actividad del canal de denuncias" en el que se incluirá la siguiente información:

1. Actividad registrada en el año anterior.
2. Resultados y conclusiones ofrecidos por los indicadores establecidos para el ejercicio anterior.
3. Objetivos e indicadores del Sistema interno de información para el ejercicio siguiente.
   Los indicadores serán del tipo: número de denuncias o informaciones recibidas, clasificación por tipología, grado de implantación y uso del canal, etc.

Se realizará un seguimiento y monitorización automatizado de estos objetivos y sus indicadores resultantes a través de la Plataforma Digital NormaPro.

IX. ANEXOS, FORMATOS Y OTROS DOCUMENTOS DE REFERENCIA

- Ev01-PGCP.06 "Política del Sistema Interno de información (canal de denuncias)".
- FOR-01-PGCP-06 "Formulario de comunicación de denuncia".
- FOR02-PGCP-06 "Derechos del denunciante en materia de protección de datos".

- FOR03-PGCP-06 “Libro Registro de Informaciones recibidas”.
- Ev06-PGCP.07 “Informe anual de Compliance para revisión por la Dirección”.
- Ev03-PGCP-06 “actividad del canal de denuncias”.