

# POLÍTICA DEL SISTEMA INTERNO DE INFORMACIÓN

Canal de Denuncias «Ley 2/2023»

## 1. PRESENTACIÓN

---

**S2a Integral Services of Audit, S.L.**, en cumplimiento de lo establecido 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, ha establecido el presente **Sistema Interno de Información** (en adelante, "el Canal").

El Canal es un medio confidencial y seguro a través del cual los trabajadores, colaboradores y terceros vinculados a la organización pueden comunicar posibles incumplimientos o irregularidades, garantizando:

- Confidencialidad absoluta de la identidad del informante.
- Presunción de inocencia de las personas señaladas.
- Disponibilidad permanente (24 horas, 7 días a la semana).
- Acceso seguro mediante encriptación AES-256-GCM y autenticación de dos factores (2FA).

## 2. PRINCIPIOS INSPIRADORES

---

El Sistema Interno de Información se rige por los siguientes principios:

### 2.1 Accesibilidad

El Canal está disponible permanentemente a través de **canal.s2auditecnia.com**, accesible desde cualquier dispositivo con conexión a Internet.

### 2.2 Transparencia

Esta política y el procedimiento de gestión están publicados y disponibles para todo el personal y terceros vinculados.

### 2.3 Buena fe

Las comunicaciones deben realizarse de buena fe, con la convicción razonable de que los hechos comunicados son ciertos.

### 2.4 Confidencialidad

- Datos personales del informante encriptados con AES-256-GCM.
- Acceso restringido mediante autenticación de dos factores (2FA).

- Protección CSRF en todos los formularios.
- Registro de auditoría completo de todos los accesos.

### *2.5 Imparcialidad*

Todas las comunicaciones se tramitan con absoluta objetividad, respetando la presunción de inocencia.

### *2.6 Eficiencia*

Las comunicaciones se tramitan con la máxima diligencia posible.

### *2.7 Seguridad técnica*

El sistema implementa medidas de alto nivel:

- Encriptación AES-256-GCM.
- 2FA para administradores.
- Protección CSRF.
- Validación exhaustiva de archivos adjuntos.
- Registro de auditoría (audit\_log).
- Control de acceso basado en roles.

## **3. ÁMBITO DE APLICACIÓN**

---

### *3.1 Ámbito material*

Pueden comunicarse a través del Canal:

#### **a) Infracciones del Derecho de la Unión Europea:**

- Contratación pública.
- Servicios, productos y mercados financieros.
- Prevención del blanqueo de capitales.
- Seguridad de los productos.
- Seguridad del transporte.
- Protección del medio ambiente.
- Protección de datos personales y privacidad.
- Seguridad de las redes.
- Protección de los intereses financieros de la Unión.
- Mercado interior.
- Cualquier otra materia del ámbito de aplicación de la Directiva (UE) 2019/1937.

#### **b) Infracciones penales o administrativas graves o muy graves**

#### **c) Incumplimientos del código ético o de la normativa interna de la organización**

### 3.2 *Ámbito personal*

Pueden utilizar el Canal:

- Trabajadores por cuenta ajena.
- Trabajadores autónomos.
- Accionistas y personas pertenecientes al órgano de administración.
- Voluntarios y personas en practices.
- Personas que trabajen bajo supervisión y dirección de contratistas, subcontratistas y proveedores.
- Personas cuya relación laboral o mercantil ya haya finalizado.

## 4. PROCEDIMIENTO DE GESTIÓN

---

### 4.1 *Presentación de la comunicación*

#### 4.1.1 Acceso al sistema

- URL: **canal.s2auditecnia.com**
- Disponibilidad: 24/7

#### 4.1.2 Pantalla informativa previa

Antes de acceder al formulario, el usuario debe leer obligatoriamente una pantalla informativa sobre:

- Naturaleza del Sistema Interno de Información.
- Ámbito de aplicación.
- Garantías de confidencialidad.
- Prohibición de comunicaciones falsas.

#### 4.1.3 Formulario multi-paso

El formulario consta de 4 pasos:

**1. Selección de categoría (obligatorio)**

**2. Identidad del denunciante:**

- Anónimo: No se solicitan datos personales.
- Identificado: Nombre completo + Email (ambos obligatorios).

**3. Descripción de los hechos (mínimo 30 caracteres, máximo 20.000)**

**4. Archivos adjuntos (opcional):**

- Máximo 5 archivos.
- Tamaño total: 15 MB.
- Formatos: PDF, DOCX, ZIP, JPG, PNG.

#### 4.1.4 Generación de identificadores

Tras enviar la comunicación, el sistema genera automáticamente:

- Código de expediente: Formato EXPnnnnnn (6 dígitos)
- Token de consulta: 64 caracteres hexadecimales

**IMPORTANTE:** El token es necesario para consultar el expediente posteriormente. El informante debe guardarlo en lugar seguro.

#### 4.2 Acuse de recibo

##### **Envío automático:**

El acuse de recibo se envía **INMEDIATAMENTE** tras crear el expediente.

##### **Condiciones:**

- Solo para comunicaciones identificadas con email.
- No se envía a comunicaciones anónimas.

##### **Contenido del acuse:**

- Confirmación de recepción.
- Código de expediente.

**Nota:** El acuse NO incluye plazos, procedimiento detallado ni token de consulta.

#### 4.3 Consulta del expediente

El informante puede consultar su expediente usando:

1. Código de expediente (EXPnnnnnn)
2. Token de consulta (64 caracteres)

##### **Seguridad:**

- Rate limiting: 5 intentos cada 5 minutos.
- Sin el token, no es posible acceder al expediente.

##### **Información visible:**

- Estado actual.
- Categoría.
- Fecha de presentación.



- Comunicaciones con el responsable.

#### *4.4 Admisión a trámite*

El Responsable del Sistema evalúa la admisibilidad de cada comunicación:

##### **Criterios de admisión:**

- Pertenece al ámbito material del Canal.
- Contiene información suficiente.
- Se presenta de buena fe.
- No es manifiestamente infundada.

##### **Criterios de inadmisión:**

- Fuera del ámbito de aplicación
- Manifiestamente infundada o falsa
- Basada en rumores
- Contenido vejatorio
- Queja laboral individual

##### **Estados del sistema:**

1. No procesado
2. En revisión
3. Revisado
4. Finalizado
5. No procede

#### *4.5 Instrucción e investigación*

##### **Actuaciones posibles:**

- Análisis documental.
- Entrevistas (informante, afectados, testigos).
- Informes técnicos.
- Otras diligencias necesarias.

##### **Comunicación bidireccional:**

El sistema permite intercambio de comentarios entre el informante y el responsable.

##### **Garantías del informante:**

- Confidencialidad absoluta.
- Protección ante represalias.
- Seguimiento del estado.

- Posibilidad de aportar información adicional.

**Garantías de las personas afectadas:**

- Presunción de Inocencia.
- Derecho a ser oído.
- Derecho a aportar pruebas.
- Derecho a conocer los hechos que se le imputan.
- No se revela la identidad del informante.

#### 4.6 Resolución

El Responsable elabora un informe final que contiene:

- Resumen de los hechos.
- Diligencias practicadas.
- Valoración jurídica.
- Conclusión.
- Propuesta de medidas (si procede).

**Medidas posibles:**

- Medidas correctivas.
- Medidas disciplinarias.
- Mejoras en procedimientos.
- Comunicación a autoridades (si procede).

**Comunicación al informante:**

- Identificado: Email con información general sobre conclusiones.
- Anónimo: Información disponible en el sistema (con expediente + token).

**Cierre del expediente:**

El expediente se cierra cuando:

- Se han adoptado las medidas necesarias.
- Se ha verificado su implementación.
- No quedan actuaciones pendientes.



## 5. CONSERVACIÓN DE DATOS

---

### 5.1 Durante la tramitación

Los datos se conservan el tiempo necesario para la investigación y adopción de medidas.

### 5.2 Anonimización automática

#### Condiciones actuales del sistema:

- Se aplica a comunicaciones en estado "No procede" o "Finalizado".
- Antigüedad: Más de 3 meses desde la fecha de presentación.
- Solo comunicaciones identificadas.

#### Proceso:

- Se eliminan: nombre, email, IP, dirección User Agent.
- Se mantienen: expediente, texto, archivos adjuntos, comentarios.

#### Anonimización inteligente por estado:

- Estados cerrados (Finalizado, No procede): Anonimización AUTOMÁTICA a los 3 meses sin intervención del responsable.
- Estados en proceso (No procesado, En revisión, Revisado): El sistema muestra avisos visuales cuando quedan menos de 10 días para la anonimización automática. El responsable puede posponer la anonimización 30 días adicionales si la investigación sigue activa.

**Sistema de avisos:** El panel administrativo incluye indicadores visuales (círculos naranjas y rojos) que alertan sobre denuncias próximas a anonimizarse, permitiendo una gestión proactiva.

### 5.3 Eliminación definitiva

- Plazo: 10 años desde la fecha de presentación
- Aplica a: TODAS las comunicaciones (cualquier estado)
- Se elimina:
  - Registro completo de la comunicación.
  - Todos los archivos adjuntos.
  - Todos los comentarios asociados.

#### Se conserva permanentemente:

- Registros de auditoría (audit\_log)
- Estadísticas anónimas

#### 5.4 Comunicaciones no tramitadas

Las comunicaciones inadmitidas se conservan 3 meses en estado anonimizado.

#### 5.5 Excepciones

Si existen indicios de delito, los datos se conservan sin anonimizar el tiempo necesario para remitirlos a las autoridades competentes.

## 6. MEDIDAS DE PROTECCIÓN

---

### 6.1 Protección del informante

#### **Confidencialidad:**

- Encriptación AES-256-GCM de datos personales.
- Acceso restringido con 2FA.
- No revelación a personas afectadas.
- Comunicación a autoridades solo si es legalmente obligatorio.

#### **Protección ante represalias:**

Prohibidas todas las represalias conforme al Capítulo III de la Ley 2/2023:

- Despido, suspensión, degradación.
- Denegación de ascenso o formación.
- Cambio de funciones, horario o ubicación.
- Reducción salarial.
- Coerción, intimidación, acoso.
- Discriminación o trato desfavorable.
- Daño reputacional.

#### **Inversión de la carga de la prueba:**

Cualquier trato desfavorable en los 2 años siguientes a la comunicación se presume represalia.

### 6.2 Protección de las personas afectadas

- Derecho a la tutela judicial efectiva.
- Presunción de Inocencia.
- Derecho de defensa.
- Derecho de acceso al expediente (excepto identidad del informante).
- Protección de su reputación e imagen.



## 7. PROTECCIÓN DE DATOS

---

### 7.1 Normativa aplicable

- Reglamento (UE) 2016/679 (RGPD)
- Ley Orgánica 3/2018 (LOPDGDD)
- Ley 2/2023

### 7.2 Responsable del tratamiento

**S2a Integral Services of Audit, S.L.**

**CIF:** B23711021

**Dirección:** Calle Doctor Pío Aguirre Rodríguez, N1, Esc1, 5A, Jaén (Andalucía) CP 23009

**Email:** administracion@s2auditecnia.com

### 7.3 Medidas de seguridad de alto nivel

#### Técnicas:

- Encriptación AES-256-GCM.
- Autenticación dos factores (2FA) con TOTP.
- Códigos de recuperación 2FA (8 caracteres).
- Protección CSRF.
- Rate limiting.
- Validación exhaustiva de archivos.
- Registro de auditoría complete.
- Sesiones seguras con cookies httpOnly.

#### Organizativas:

- Acceso restringido a personal autorizado.
- Formación específica del personal.
- Compromisos de confidencialidad.
- Revisiones periódicas.
- Control físico de acceso a servidores.

## 8. FORMACIÓN Y DIFUSIÓN

---

### 8.1 Formación

El personal responsable del Canal recibe formación específica sobre:

- Ley 2/2023
- RGPD y LOPDGDD



- Procedimientos del Canal
- Medidas de seguridad

### 8.2 Difusión

Esta política se comunica a través de:

- Web corporative.
- Intranet.
- Contratos laborales.
- Circulares informativas.

## 9. REVISIÓN Y MEJORA

---

Esta política se revisa:

- Como mínimo, anualmente.
- Tras cambios normativos.
- Tras incidentes significativos.
- A propuesta del Responsable del Sistema.

## 10. ENTRADA EN VIGOR

---

Esta política entra en vigor el 08/04/2026 tras su aprobación por la Dirección de S2a Integral Services of Audit, S.L.

### Aprobado por:

Salvador Sánchez Jiménez

**Fecha:** 08/04/2026

**Última actualización:** 08/04/2026