# POLÍTICA DE PROTECCIÓN DE DATOS

Sistema Interno de Información (Canal de Denuncias)

## 1. RESPONSABLE DEL TRATAMIENTO

**AUDICIDAD GLOBAL, S.L.P**

**CIF:** B05515945

**Dirección:** Calle Norte, nº 100, de Molina de Segura (Murcia), con C.P. 30.500

**Email:** anabelen@audicidad.com

## 2. FINALIDAD DEL TRATAMIENTO

Los datos personales recabados a través del Sistema Interno de Información se tratan con las siguientes finalidades:

- Cumplimiento de las obligaciones legales derivadas de la Ley 2/2023.
- Gestión y tramitación de las comunicaciones recibidas.
- Investigación de los hechos comunicados.
- Adopción de medidas correctivas o disciplinarias.
- Protección de los intereses de la organización y sus empleados.
- Prevención de infracciones normativas.

## 3. CATEGORÍAS DE DATOS TRATADOS

### *3.1 Datos del informante (si identificado)*

**Datos recopilados:**

- Identificativos: nombre complete.
- Contacto: dirección de correo electrónico.
- Datos técnicos: dirección IP, User Agent.

**Tratamiento especial:**

- Nombre y email se encriptan con AES-256-GCM antes de almacenar.
- IP y User Agent se almacenan sin encriptar para fines de seguridad.

- Generación de código de expediente (EXPnnnnnn).
- Generación de token de consulta (64 caracteres hexadecimales).

**Nota:** En comunicaciones anónimas no se recaban datos personales.

### *3.2 Datos del contenido de la comunicación*

- Categoría de la infracción.
- Descripción de los hechos (texto libre).
- Archivos adjuntos (documentos, imágenes).
- Fecha y hora de presentación.

### *3.3 Datos de las personas afectadas*

Pueden aparecer en la descripción:

- Identificativos.
- Datos de contacto.
- Características personales.
- Datos académicos y profesionales.
- Datos de Empleo.
- Datos económicos y financieros.
- Potencialmente, categorías especiales de datos (si son relevantes para la infracción).

### *3.4 Datos de terceros (testigos, otros)*

- Identificativos.
- Datos de contacto.
- Declaraciones o testimonios.

## 4. FUENTES DE LOS DATOS

### *4.1 Datos del informante*

**Fuente:** Directamente del interesado a través del formulario web del Sistema Interno de Información.

### *4.2 Datos de personas afectadas y terceros*

**Fuente:** De la propia comunicación y del proceso de investigación.

## 5. LEGITIMACIÓN DEL TRATAMIENTO

**Base jurídica:** Obligación legal (artículo 6.1.c del RGPD)

El tratamiento es necesario para el cumplimiento 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.

**No se requiere consentimiento** del interesado para el tratamiento de sus datos en este contexto.

## 6. CESIONES Y COMUNICACIONES DE DATOS

Los datos podrán comunicarse a:

### *6.1 Autoridades públicas*

- Ministerio Fiscal y autoridades judiciales: Si se detectan indicios de delito.
- Defensor del Pueblo: Si la comunicación se deriva al canal externo.
- Tribunal de Cuentas: Si procede la derivación.
- Autoridades administrativas competentes: Si existen infracciones administrativas.

### *6.2 Profesionales externos*

- Peritos o expertos: Para la elaboración de informes técnicos.
- Estos profesionales suscriben acuerdos de confidencialidad.

### *6.3 No se realizan transferencias internacionales de datos*

## 7. PLAZOS DE CONSERVACIÓN

### *7.1 Durante la tramitación*

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

### *7.2 Tras el cierre del expediente*

**Anonimización AUTOMÁTICA:**

- Proceso: Se eliminan nombre, email, IP y User Agent encriptados.
- Se mantiene: Expediente, texto, archivos, comentarios

Anonimización inteligente:

- Estados cerrados (Finalizado, No procede):
  - Anonimización AUTOMÁTICA a los 3 meses.
  - Sin intervención necesaria del responsible.
  - Garantiza cumplimiento normative.
- Estados en proceso (No procesado, En revisión, Revisado):
  - Avisos visuales cuando quedan <10 días.
  - Posibilidad de posponer 30 días si la investigación está active.
  - Anonimización automática si no se postpone.

El sistema incluye indicadores visuales en el panel administrativo para facilitar la gestión proactiva de los plazos de anonimización.

**Eliminación definitiva:**

- Plazo: 10 años desde la fecha de presentación.
- Se elimina: Todo el expediente, archivos y comentarios asociados.
- Se conserva: Registros de auditoría (audit_log) de forma permanente.

### *7.3 Excepciones*

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

## 8. MEDIDAS DE SEGURIDAD

### *8.1 Medidas técnicas*

**Encriptación:**

- Algoritmo: AES-256-GCM (Galois/Counter Mode).
- Datos encriptados: Nombre y email del informante (si identificado).
- Claves: Única por instalación, almacenada en .env
- HTTPS: Todas las comunicaciones web encriptadas.

**Control de acceso:**

- Autenticación: 2FA obligatorio (TOTP) para administradores.
- Códigos de recuperación: 8 caracteres alfanuméricos (10 códigos).
- Gestión de sesiones: Cookies httpOnly, secure, samesite=strict.
- Contraseñas: Hasheadas con bcrypt.

**Protección de formularios:**

- CSRF protection: Token único por session.
- Honeypot: Campo oculto anti-bots.
- Rate limiting: Límites por IP/sesión.
- Validación exhaustiva: Todos los campos.

**Registro de auditoría:**

- Tabla audit_log: Todas las acciones registradas.
- Información: user_id, action, subject_id, meta (JSON), IP, timestamp.
- Conservación: Permanente.

**Validación de archivos:**

- MIME real: Verificación con finfo_file.
- Extensión: Lista blanca (PDF, DOCX, ZIP, JPG, PNG).
- Tamaño: Máximo 15 MB total.
- Almacenamiento: Nombres hasheados, permisos restringidos.

**Claves de seguridad:**

- ENCRYPTION_KEY: 64 caracteres hexadecimales.
- SESSION_SECRET: 64 caracteres hexadecimales.
- Única por instalación.

### *8.2 Medidas organizativas*

**Acceso restringido:**

- Solo personal autorizado y formado.
- Principio de necesidad de conocer.
- Registro de todos los accesos en audit_log.
- Revisiones periódicas de accesos.

**Compromisos de confidencialidad:**

- Firmados por todo el personal con acceso.
- Obligación permanente, incluso tras finalizar la relación.
- Consecuencias del incumplimiento claramente establecidas.

**Formación:**

- Inicial obligatoria para personal responsible.
- Actualizaciones periódicas.

- Protección de datos y Ley 2/2023.

**Medidas físicas:**

- Acceso controlado a servidores.
- Estaciones de trabajo protegidas.
- Bloqueo automático de sesiones.
- Destrucción segura de documentos físicos.

### *8.3 Garantías de confidencialidad*

**Del informante:**

- Identidad solo conocida por el Responsable del Sistema.
- Datos encriptados en base de datos.
- No revelación a personas afectadas.
- Comunicación a autoridades solo si legalmente obligatorio.

**De las personas afectadas:**

- Datos solo utilizados para la investigación.
- No divulgación innecesaria.
- Protección de la reputación.
- Presunción de inocencia en todo momento.

**De terceros (testigos):**

- Protección de sus datos personales.
- Uso exclusivo para la investigación.
- Confidencialidad de sus declaraciones.

## 9. DERECHOS DE LOS INTERESADOS

### *9.1 Derechos reconocidos*

Conforme al RGPD, los interesados tienen derecho a:

- Acceso: Obtener información sobre sus datos tratados.
- Rectificación: Corregir datos inexactos.
- Supresión ("derecho al olvido"): En determinadas circunstancias.
- Limitación del tratamiento: En casos específicos.
- Oposición: Al tratamiento de sus datos.
- Portabilidad: Recibir sus datos en formato estructurado.
- No ser objeto de decisiones automatizadas.

### *9.2 Limitaciones específicas*

**Para el informante:**

- Puede ejercer todos sus derechos.
- Supresión limitada durante la tramitación (obligación legal de conservación).
- Tras cierre: anonimización automática según plazos establecidos.

**Para las personas afectadas:**

- Pueden acceder a sus datos.
- NO pueden acceder a la identidad del informante.
- Ejercicio de derechos compatible con garantías del informante.

### *9.3 Ejercicio de derechos*

**Medios:**

- Email: anabelen@audicidad.com
- Postal: Calle Norte, nº 100, de Molina de Segura (Murcia), con C.P. 30.500

**Documentación requerida:**

- Solicitud identificando claramente el derecho a ejercer
- Copia del DNI o documento equivalente

**Plazo de respuesta:**

- Máximo 1 mes desde la recepción de la solicitud
- Ampliable 2 meses más si es necesario (con justificación)

## 10. RECLAMACIONES

Si el interesado considera que el tratamiento de sus datos vulnera la normativa, puede presentar reclamación ante:

**Agencia Española de Protección de Datos (AEPD)**

**Web:** www.aepd.es

**Dirección:** C/ Jorge Juan, 6, 28001 Madrid

**Teléfono:** 901 100 099 / 912 663 517

## 11. INFORMACIÓN ADICIONAL

Para información más detallada sobre el tratamiento de datos en el Sistema Interno de Información, consulte:

- Política del Sistema Interno de Información.
- Procedimiento de Gestión del Canal de Denuncias.

Estos documentos están disponibles en la pantalla informativa previa al formulario.

## 12. ACTUALIZACIÓN DE LA POLÍTICA

Esta política se revisa periódicamente para asegurar su conformidad con la normativa vigente y las mejores prácticas en protección de datos.

**Aprobado por:**

Ana Belén Ortuño Caballero

Responsable del Canal

**Fecha:** 08/04/2026

**Última actualización:** 08/04/2026