



GRUP D'EDUCADORS
DE CARRER I TREBALL
AMB MENORS

ESPECIFICACIONES TÉCNICAS DE GARANTÍA DE ANONIMATO

Canal de Denuncias del Grec

Documento técnico conforme 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.

Contenido

1. Introducción y marco legal
2. Arquitectura del sistema
3. Datos que NO se almacenan
4. Datos que SÍ se almacenan
5. Sistema de identificación de denuncias
6. Encriptación de datos sensibles
7. Comunicación bidireccional anónima
8. Tratamiento de archivos adjuntos
9. Medidas de seguridad adicionales
10. Certificación de cumplimiento

1. INTRODUCCIÓN Y MARCO LEGAL

El presente documento describe las especificaciones técnicas implementadas en el Canal de Denuncias del Grec para garantizar el anonimato de las personas denunciantes, en cumplimiento 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.
- Reglamento (UE) 2016/679 (RGPD) relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.
- Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

El sistema ha sido diseñado con el principio de "privacidad por diseño" (Privacy by Design), garantizando que la protección del anonimato es una característica intrínseca de la arquitectura, no una funcionalidad añadida.

2. ARQUITECTURA DEL SISTEMA

El Canal de Denuncias es un sistema web independiente que:

- NO utiliza servicios de terceros para el procesamiento de denuncias
- NO comparte datos con plataformas externas
- Almacena todos los datos en servidores propios ubicados en la UE
- Opera bajo protocolo HTTPS con certificado SSL/TLS

Componentes principales:

- Formulario público de envío de denuncias
- Sistema de consulta mediante código de seguimiento
- Panel de administración para gestión de expedientes
- Sistema de mensajería bidireccional segura

3. DATOS QUE NO SE ALMACENAN

El sistema está configurado técnicamente para NO registrar ni almacenar:

3.1 DIRECCIÓN IP

El sistema NO registra la dirección IP del dispositivo desde el que se realiza la denuncia. Esta medida se implementa a nivel de aplicación, no dependiendo de la configuración del servidor web.

Las denuncias anónimas no contienen ninguna referencia a la IP de origen en ningún campo de la base de datos.

3.2 DATOS DEL NAVEGADOR (USER-AGENT)

NO se almacena información sobre:

- Tipo de navegador utilizado
- Versión del navegador
- Sistema operativo
- Resolución de pantalla
- Plugins instalados

3.3 MARCAS DE TIEMPO PRECISAS

Para denuncias anónimas, únicamente se registra la FECHA (día/mes/año), nunca la hora exacta. Esto impide correlacionar la denuncia con registros de acceso del servidor web.

Formato almacenado: DATE (ej: 2026-01-23)

NO se almacena: DATETIME ni TIMESTAMP

3.4 COOKIES IDENTIFICATIVAS

El sistema no utiliza cookies de seguimiento ni cookies persistentes que permitan identificar al usuario entre sesiones.

Únicamente se utilizan cookies de sesión técnicas, necesarias para el funcionamiento del formulario, que se eliminan al cerrar el navegador.

3.5 DATOS DE GEOLOCALIZACIÓN

NO se solicita ni se almacena ninguna información geográfica del usuario.



4. DATOS QUE SÍ SE ALMACENAN

Para denuncias ANÓNIMAS, únicamente se almacena:

DATO	PROPÓSITO
Descripción (cifrada)	Contenido de la denuncia
Fecha de creación	Solo fecha, sin hora
Fecha de los hechos	Opcional, proporcionada por el usuario
Categoría	Clasificación de la denuncia
Estado del expediente	Seguimiento del proceso
Hash del código	Identificación sin almacenar el código

Para denuncias IDENTIFICADAS (cuando el usuario decide voluntariamente proporcionar sus datos), adicionalmente se almacena:

DATO	PROPÓSITO
Nombre (cifrado)	Contacto con el denunciante
Email (cifrado)	Notificaciones automáticas

IMPORTANTE: La decisión de identificarse es VOLUNTARIA.

5. SISTEMA DE IDENTIFICACIÓN DE DENUNCIAS

5.1 CÓDIGO DE SEGUIMIENTO

Cada denuncia recibe un código único con formato: GR3C-XXXX-XXXX-XXXX

Este código se genera mediante:

- Función: random_bytes(16) de PHP
- Entropía: 128 bits de aleatoriedad criptográfica
- Formato: Base62 (letras mayúsculas y números)

Ejemplo: GR3C-7K9M-P2QR-4XYZ

5.2 ALMACENAMIENTO SEGURO DEL CÓDIGO

El código de seguimiento NUNCA se almacena en texto plano.

En la base de datos se guarda únicamente un HASH SHA-256 del código:

```
hash('sha256', 'GR3C-7K9M-P2QR-4XYZ')  
= "a3f2b8c9d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8a9b0c1d2e3f4a5b6c7d8e9f0a1"
```

Esto significa que:

- Es IMPOSIBLE obtener el código original a partir del hash
- Solo quien posee el código puede consultar su denuncia
- Ni siquiera los administradores pueden ver los códigos

5.3 VERIFICACIÓN DE ACCESO

Cuando un usuario introduce su código para consultar el estado:

1. El sistema calcula el hash del código introducido
2. Busca en la base de datos una coincidencia del hash
3. Si coincide, muestra los datos de la denuncia
4. Si no coincide, muestra un error genérico

Este proceso no revela si el código existe o no (protección contra ataques de enumeración).

6. ENCRIPCIÓN DE DATOS SENSIBLES

6.1 ALGORITMO UTILIZADO

Todos los datos sensibles se cifran con:

- Algoritmo: AES-256-CBC
- Longitud de clave: 256 bits
- Modo: CBC (Cipher Block Chaining)

6.2 DATOS CIFRADOS

Se cifran mediante AES-256:

- Descripción de los hechos
- Información adicional
- Nombre del denunciante (si se identifica)
- Email del denunciante (si se identifica)
- Contenido de los mensajes
- Notas internas de los administradores

6.3 VECTOR DE INICIALIZACIÓN (IV)

Cada campo cifrado utiliza un IV único generado aleatoriamente:

- Generación: random_bytes(16)
- Almacenamiento: junto al dato cifrado (separado)
- Reutilización: NINGUNA (IV nuevo para cada operación)

6.4 GESTIÓN DE LA CLAVE

La clave de encriptación:

- Se almacena en archivo de configuración fuera del directorio web
- NO es accesible desde internet
- Solo es conocida por los administradores del sistema

7. COMUNICACIÓN BIDIRECCIONAL ANÓNIMA

7.1 SISTEMA DE MENSAJERÍA

El sistema permite comunicación entre el denunciante y los administradores sin comprometer el anonimato:

- Los mensajes se envían a través del código de seguimiento
- El denunciante no necesita revelar su identidad para comunicarse
- Todos los mensajes se cifran con AES-256

7.2 NOTIFICACIONES

Para denuncias ANÓNIMAS:

- No hay notificaciones automáticas (no hay email)
- El denunciante debe consultar activamente con su código de seguimiento

Para denuncias IDENTIFICADAS:

- Se envían notificaciones por email cuando hay novedades en el expediente

8. TRATAMIENTO DE ARCHIVOS ADJUNTOS

8.1 SANITIZACIÓN DE METADATOS

Todos los archivos adjuntos son procesados para eliminar metadatos que podrían identificar al remitente:

IMÁGENES (JPG, PNG, GIF):

- Eliminación de datos EXIF (GPS, cámara, fecha, autor)
- Eliminación de miniaturas incrustadas
- Eliminación de perfiles de color con información personal

DOCUMENTOS (PDF, DOC, DOCX, XLS, XLSX):

- Se notifica al usuario sobre la existencia de metadatos
- Se recomienda usar versiones "limpias" de los documentos

8.2 ALMACENAMIENTO SEGURO

- Los archivos se renombran con UUID aleatorio
- Se almacenan fuera del directorio web público
- Acceso solo mediante verificación del código de seguimiento

9. MEDIDAS DE SEGURIDAD ADICIONALES

9.1 PROTECCIÓN CONTRA ATAQUES

- Protección CSRF con tokens de sesión
- Prevención de inyección SQL con consultas parametrizadas
- Escapado de salida HTML (prevención XSS)
- Rate limiting para prevenir ataques de fuerza bruta

9.2 SEGURIDAD DEL PANEL DE ADMINISTRACIÓN

- Autenticación con Argon2id (hash de contraseñas)
- Bloqueo tras 5 intentos fallidos
- Sesiones con expiración automática
- URL no enlazada desde la web pública

9.3 REGISTROS DEL SISTEMA

Los logs del sistema:

- NO registran direcciones IP de denunciantes
- NO registran códigos de seguimiento
- Solo registran eventos técnicos (errores, accesos admin)

10. CERTIFICACIÓN DE CUMPLIMIENTO

DECLARACIÓN TÉCNICA:

El sistema de Canal de Denuncias del Grec ha sido diseñado e implementado siguiendo los principios de privacidad por diseño y minimización de datos.

Certificamos que:

1. El sistema NO PUEDE identificar a un denunciante anónimo porque no almacena ningún dato identificativo (IP, navegador, hora exacta).
2. El código de seguimiento es la ÚNICA forma de acceder a una denuncia, y este código no se almacena en texto plano en ningún lugar.
3. Todos los datos sensibles están cifrados con AES-256, algoritmo considerado seguro por los estándares internacionales.
4. Los archivos adjuntos son procesados para eliminar metadatos que podrían comprometer el anonimato.
5. El sistema cumple con los requisitos técnicos establecidos en la Ley 2/2023 para canales de denuncia internos.