CanaryTek

SEGURIDAD DE LA INFORMACIÓN

CanaryTek Canal del Informante

Índice

1. Resumen ejecutivo

CanaryTek Canal del Informante está diseñado para maximizar la protección de la persona informante y reducir la superficie de exposición de datos sensibles durante todo el ciclo de vida de una comunicación.

La plataforma aplica un enfoque de privacidad por diseño, criptografía de extremo a extremo y minimización de metadatos, con controles orientados a evitar la correlación entre denuncias.

Su diseño funcional y técnico está orientado al 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, y se alinea con los principios de la Directiva (UE) 2019/1937.

2. Marco normativo de referencia

Este dossier se formula tomando como referencia el marco jurídico aplicable en España y la Unión Europea, en particular:

- 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 (UE) 2019/1937 del Parlamento Europeo y del Consejo, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.
- Reglamento (UE) 2016/679 (RGPD) y Ley Orgánica 3/2018 (LOPDGDD), en lo relativo a principios de licitud, minimización, seguridad e integridad del tratamiento.

La solución no sustituye al asesoramiento jurídico específico de la organización, pero facilita la implantación de controles técnicos y organizativos coherentes con las exigencias de confidencialidad, trazabilidad y protección de la persona informante.

3. Objetivos de seguridad y privacidad

Los objetivos principales, desde una perspectiva de cumplimiento normativo, son:

- proteger la identidad de la persona informante;
- impedir el acceso al contenido por parte de operadores de infraestructura;
- limitar metadatos que puedan facilitar identificación indirecta;
- preservar la integridad y trazabilidad del expediente;
- reducir el riesgo de correlación entre denuncias independientes.

4. Arquitectura de protección de la persona informante

4.1. Cifrado de extremo a extremo

Las comunicaciones del informante se cifran en cliente antes de salir del dispositivo.

- El contenido se cifra con la clave pública del RPI.
- El servidor API actúa como almacenamiento opaco y no necesita acceso al contenido en claro.
- Las respuestas del RPI se cifran para la clave pública asociada a la denuncia.

Este esquema evita que terceros con acceso a infraestructura puedan leer el contenido funcional del expediente.

Desde una perspectiva legal, este enfoque refuerza la obligación de confidencialidad y la protección efectiva de la identidad de la persona informante durante la tramitación.

4.2. Claves independientes por denuncia

Para reducir la correlación entre comunicaciones, cada denuncia se gestiona con material criptográfico independiente.

- Se evita reutilizar una misma identidad criptográfica para todas las denuncias.
- Se limita la posibilidad de vincular varias denuncias al mismo origen por patrones de clave.

4.3. Segmentación por canal

Cada canal opera con aislamiento lógico de datos.

- Las operaciones administrativas se acotan a su canal.
- Los accesos de RPI se restringen al ámbito de su canal.

Esta segmentación contribuye al principio de necesidad de acceso y reduce el riesgo de accesos no autorizados o de tratamiento excesivo de información.

5. Política de adjuntos y metadatos

5.1. Principios aplicados

La plataforma aplica minimización de metadatos en adjuntos, conforme al principio de minimización de datos:

- el nombre original del archivo no se conserva;

- se genera un nombre anónimo derivado de hash;
- se conserva tipo MIME y tamaño porque son necesarios para gestión funcional del expediente;
- se guarda hash de contenido para trazabilidad técnica.

5.2. Limpieza de metadatos en adjuntos

La limpieza se aplica en modo best-effort.

- En imágenes, se realiza reprocesado para reducir metadatos embebidos habituales.
- En otros formatos (por ejemplo, ofimática compleja), no es posible garantizar eliminación total de metadatos internos en todos los casos.

Por ese motivo, la interfaz informa explícitamente de los límites de garantía en la eliminación total de metadatos.

5.3. Políticas operativas de adjuntos

La plataforma permite dos políticas configurables en runtime:

- **best-effort**: mayor flexibilidad de formatos con limpieza best-effort;
- **strict**: restringe adjuntos a imágenes y PDF para reducir riesgo operativo.

En escenarios con mayores exigencias de cumplimiento o sensibilidad, se recomienda política **strict** como configuración preferente.

6. Minimización de datos y exposición

- No se requiere exponer nombre real de ficheros adjuntos.
- Se evita recopilar información no necesaria para tramitar la comunicación.
- Se limita la persistencia local al mínimo necesario para continuidad del hilo.

7. Integridad, continuidad y custodia

- El expediente mantiene secuencia de mensajes cifrados.
- Se contemplan mecanismos de backup y restauración del canal.
- El RPI conserva capacidad de seguimiento con trazabilidad operacional.

Estos controles facilitan la acreditación de diligencia en la gestión del canal y la conservación ordenada de evidencias para auditoría interna o requerimiento de autoridad competente.

8. Limitaciones y consideraciones

Ningún sistema puede ofrecer riesgo cero. Esta solución reduce sustancialmente el riesgo de identificación y filtración de contenido, pero se recomienda complementar con:

- políticas internas de uso seguro;
- formación de usuarios y RPI;
- revisiones periódicas de configuración;
- controles de gobierno y auditoría.

Asimismo, se recomienda disponer de protocolo interno de gestión del canal, políticas de conservación y borrado, y registro de actuaciones del RPI conforme al marco legal aplicable.

9. Recomendaciones de implantación

Para maximizar la protección del informante se recomienda:

- activar políticas de adjuntos en modo **strict** cuando sea viable;
- documentar el procedimiento interno de recepción y gestión de denuncias;
- rotar credenciales operativas y revisar permisos periódicamente;
- mantener actualizado el entorno de despliegue y dependencias.
- validar periódicamente la adecuación jurídica y técnica del canal frente a cambios normativos.

10. Matriz de cumplimiento (resumen operativo)

Esta sección complementa el dossier con una vista rápida de correspondencia entre obligación legal, riesgo mitigado y control aplicado, sin sustituir al análisis jurídico específico de la organización.

Obligación legal	Riesgo mitigado	Control técnico aplicado	Evidencia de cumplimiento
Protección de la identidad de la persona informante	Identificación directa o indirecta de la persona informante	Cifrado de extremo a extremo, minimización de metadatos y anonimización de nombre de adjuntos	Configuración del canal, revisión de políticas de adjuntos y pruebas funcionales del flujo de denuncia
Confidencialidad de la comunicación	Acceso no autorizado al contenido por terceros u operadores de infraestructura	Cifrado en cliente, custodia criptográfica por rol y acceso restringido por canal	Verificación de arquitectura, trazas de acceso y controles de permisos

Obligación legal	Riesgo mitigado	Control técnico aplicado	Evidencia de cumplimiento
Integridad y trazabilidad del expediente	Alteración, pérdida o falta de secuencia en el histórico de comunicaciones	Registro ordenado de mensajes cifrados, hash de contenido y mecanismos de backup/restauración	Evidencias de restauración, registros de operación y auditoría interna
Principio de minimización de datos	Recopilación o conservación de datos no necesarios	Reducción de metadatos en adjuntos y limitación de atributos operativos a los estrictamente necesarios	Revisión periódica de configuración y documentación de medidas de minimización
Gobernanza y diligencia del responsable	Deficiencias en la tramitación y custodia del canal	Procedimientos internos, segmentación de accesos y controles de operación	Protocolo interno aprobado, registro de actuaciones y revisiones periódicas

11. Contacto

Para evaluación, implantación y personalización del canal:

- info@canarytek.com