Política de Tratamiento de Datos Personales y Anonimización de Datos Sensibles Red de Veedurías – REDVIGILA

V. 2026/01/20

Contenido

Política de Tratamiento de Datos Personales y Anonimización de Datos Sensibles Red de Veedurías

1. Propósito y enfoque

La Red Colombiana de Veedurías, REDVIGILA (en adelante, la Red) adopta la presente política para garantizar el derecho fundamental de habeas data, asegurar el tratamiento lícito, leal y transparente de los datos personales y proteger de manera reforzada los datos sensibles y los datos de niños, niñas y adolescentes (NNA), especialmente cuando la información se vincula con denuncias, quejas, actuaciones administrativas, disciplinarias y/o judiciales, donde existe riesgo de revictimización, estigmatización o represalias.

La política se fundamenta en el principio de responsabilidad demostrada *(accountability)* y en un modelo de gestión de riesgos orientado a mantener niveles aceptables de confidencialidad, integridad y disponibilidad, alineado con prácticas institucionales como la designación de un Oficial de Protección de Datos y registros de incidentes y plan de acción
.

2. Titulares de los derechos - Titulares de los datos personales.

2.1. Definición
Para efectos de esta política, Titular es toda persona natural a la que se refieren los datos personales objeto de tratamiento por parte de la Red, independientemente del canal por el cual la información se obtenga (presencial, físico, digital, telefónico o audiovisual) y sin importar si la información proviene directamente del Titular o de un tercero.
2.2. Se consideran Titulares —sin limitarse a— las siguientes personas naturales:
a) Ciudadanía y usuarios de los servicios de la Red
- Personas que presentan denuncias, quejas, peticiones, solicitudes o aportan información.
- Participantes en ejercicios de control social, audiencias, mesas de trabajo, encuestas o actividades institucionales.

b) Personas vinculadas a casos y actuaciones
- Denunciantes, peticionarios y reportantes.
- Testigos, informantes y fuentes.
- Personas presuntamente afectadas o víctimas.
- Personas mencionadas en denuncias, expedientes o actuaciones (p. ej. presuntos responsables o terceros relacionados), aun cuando no interactúen directamente con la Red.

c) Sujetos de especial protección
- Niños, niñas y adolescentes (NNA).
- Personas en condición de riesgo o vulnerabilidad (p. ej. líderes sociales, defensores de DD. HH., personas amenazadas), cuando corresponda.

d) Talento humano y vinculados institucionales
- Funcionarios/servidores, veedores vinculados, personal de apoyo.
- Contratistas (personas naturales) y su equipo, cuando aplique.

- Aspirantes a vinculación, pasantes, practicantes, judicantes y voluntarios.

e) Proveedores, aliados y contactos (personas naturales)

- Representantes legales, apoderados, interventores, supervisores, consultores.
- Contactos de entidades y organizaciones aliadas, cuando se trate de personas naturales.

2.3. Derechos de los Titulares | La Red reconoce y garantiza a los Titulares, como mínimo, los siguientes derechos:

1. Conocer, actualizar y rectificar sus datos personales.
2. Solicitar prueba de la autorización otorgada, salvo cuando exista habilitación legal.
3. Ser informado sobre el uso que se ha dado a sus datos.
4. Presentar quejas ante la SIC, una vez agotado el trámite interno de consulta o reclamo.
5. Revocar la autorización y/o solicitar la supresión del dato cuando proceda, siempre que no exista deber legal o contractual de conservarlo.
6. Acceder de forma gratuita a sus datos personales, al menos una vez por mes calendario y cada vez que existan modificaciones sustanciales de esta política, conforme a la normativa aplicable.

2.4. Legitimación para el ejercicio de derechos | Los derechos podrán ejercerse por:

- El Titular directamente.
- Sus causahabientes, cuando aplique.
- Su representante legal, en especial para NNA.
- Un apoderado debidamente acreditado.

Regla reforzada: cuando el Titular sea denunciante, testigo, víctima o NNA, la Red aplicará medidas reforzadas de confidencialidad, acceso restringido y anonimización en productos públicos.

3. Alcance y ámbito de aplicación

3.1. A quién aplica (sujetos obligados) | Esta política aplica de manera obligatoria a:

a) Integrantes de la Red

- Funcionarios y servidores públicos.
- Veedores vinculados a la Red, equipos técnicos y personal de apoyo.
- Practicantes, pasantes, judicantes, aprendices y voluntarios que accedan a información.

b) Contratistas, operadores y proveedores (encargados del tratamiento)

- Contratistas de servicios, consultores, interventores y supervisores.
- Proveedores tecnológicos (nube, hosting, software, soporte y mantenimiento).
- Operadores de canales (call center, mensajería, chat, formularios web).
- Servicios de archivo, custodia, digitalización, mensajería y logística.
- Agencias y/o equipos de comunicaciones y producción audiovisual cuando manejen casos o datos personales.

c) Terceros aliados (con acceso o recepción de datos)

- Entidades públicas y organismos de control con interacción misional.
- Organizaciones sociales, academia y cooperación.
- Peritos, auditores, traductores, expertos externos.

d) Tratamientos indirectos.
Aplica también cuando exista acceso incidental o derivado (copias, reenvíos, capturas, soporte técnico, backups, logs y metadatos).
3.2. Dónde aplica (bases, repositorios, sistemas y medios): Aplica a todas las bases de datos y repositorios físicos o digitales, incluidos, sin limitarse a:

- Recepción de denuncias, PQRS y derechos de petición.
- Expedientes misionales y administrativos.
- Correo institucional y buzones funcionales.
- Actas, informes, minutas, borradores y anexos.
- Contenidos digitales, web y redes sociales (incluye mensajes directos).
- Registros audiovisuales (foto, video, audio) y sus metadatos.
- Repositorios de evidencias, archivos físicos, bodegas documentales.
- Infraestructura tecnológica (equipos, servidores, nube, almacenamiento compartido).
- Copias de seguridad, bitácoras, registros de acceso, auditoría.

3.3. Qué datos cubre (categorías): Comprende datos de identificación, contacto, localización, socioeconómicos y laborales, sensibles, biométricos, datos de NNA, y datos digitales (IP, identificadores, metadatos) cuando sean recolectados o generados por los canales institucionales.
3.4. Qué operaciones cubre (tratamientos): | Incluye recolección, almacenamiento, uso, consulta, análisis, circulación, transmisión, transferencia, divulgación (con anonimización cuando corresponda), conservación, archivo, backup, recuperación y supresión.
3.5. Escenarios de especial sensibilidad (aplicación reforzada)
La política aplica con estándar reforzado cuando se trate de:

- Denuncias con riesgo de represalias o amenazas.
- Casos con víctimas, testigos, denunciantes o NNA.
- Procesos disciplinarios o judiciales con reserva o debido proceso.
- Contextos territoriales de alta reidentificación (poblaciones pequeñas).
- Productos de publicación, prensa o rendición de cuentas.

4. Definiciones operativas (mínimas):

Para efectos de esta política, se adoptan las siguientes definiciones, en concordancia con el régimen colombiano de protección de datos personales y los lineamientos técnicos aplicables:
4.1. Dato personal
Cualquier información vinculada o que pueda asociarse a una persona natural, directa o indirectamente. Incluye, entre otros: nombre, número de identificación, dirección, teléfono, correo, imagen, voz, placa del vehículo asociada al titular, usuario institucional, identificadores en línea y metadatos cuando permitan asociar a una persona.
4.2. Dato público
Dato calificado como público por la normativa aplicable o por su naturaleza, siempre que su tratamiento respete los principios de finalidad, circulación restringida y seguridad. Se consideran típicamente públicos: los relativos al estado civil, profesión u oficio, calidad de servidor público, y aquellos contenidos en registros públicos, sin perjuicio de la evaluación de riesgo y de las reglas de reserva y protección en contextos de denuncias o procesos.
4.3. Dato semiprivado

Dato que no es íntimo, reservado ni público, cuyo conocimiento o divulgación interesa al titular y a un sector determinado o a la sociedad en general, pero con acceso o circulación limitada (p. ej. información financiera o crediticia en ciertos contextos regulados). Su tratamiento exige medidas de control y seguridad acordes con el riesgo.

4.4. Dato privado

Dato que por su naturaleza íntima o reservada solo es relevante para el titular y su acceso debe ser restringido. Su divulgación indebida puede afectar derechos fundamentales (p. ej. domicilio, comunicaciones privadas, información familiar, historia personal).

4.5. Dato sensible

Dato personal que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación. Incluye, entre otros:

- Origen racial o étnico.
- Orientación sexual o vida sexual.
- Convicciones religiosas, filosóficas o políticas.
- Pertenencia a sindicatos, organizaciones sociales, de derechos humanos o partidos.
- Datos relativos a salud (física o mental).
- Datos biométricos (huellas, reconocimiento facial, voz biométrica, iris, etc.).
- Información sobre víctimas, denunciantes, testigos o personas en riesgo, cuando su identificación pueda generar represalias.

Regla reforzada: el tratamiento de datos sensibles se presume restrictivo y exige mayores salvaguardas, acceso limitado, justificación, y cuando aplique, autorización explícita o habilitación legal.

4.6. Datos de niños, niñas y adolescentes (NNA)

Datos personales de NNA. Su tratamiento es de carácter excepcional y debe respetar el interés superior del menor y sus derechos prevalentes. Requiere controles reforzados, minimización y, en general, anonimización estricta para divulgación o publicación.

4.7. Titular

Persona natural a quien se refieren los datos personales objeto de tratamiento.

4.8. Autorización

Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de sus datos personales, salvo las excepciones legales. Debe poder probarse y conservarse su evidencia.

4.9. Tratamiento

Cualquier operación o conjunto de operaciones sobre datos personales, tales como: recolección, almacenamiento, uso, circulación, transmisión, transferencia, actualización, supresión, consulta, análisis, divulgación o archivo.

4.10. Responsable del tratamiento

Persona natural o jurídica, pública o privada, que decide sobre la base de datos y/o el tratamiento, incluyendo sus finalidades, condiciones, medios y destinatarios.

4.11. Encargado del tratamiento

Persona natural o jurídica, pública o privada, que realiza el tratamiento por cuenta del responsable, conforme a sus instrucciones y a un contrato o instrumento vinculante.

4.12. Base de datos

Conjunto organizado de datos personales que sea objeto de tratamiento, en cualquier soporte (físico o digital), incluyendo archivos, expedientes, sistemas de PQRS, hojas de cálculo, correos funcionales, repositorios documentales y sistemas audiovisuales.

4.13. Aviso de privacidad
Comunicación verbal o escrita generada por el responsable, dirigida al titular, para informarle sobre la existencia de la política de tratamiento, la forma de acceder a ella y las finalidades principales del tratamiento, cuando no sea posible poner a disposición el texto completo en el punto de recolección.
4.14. Consulta
Solicitud del titular para conocer los datos personales que reposan en una base de datos del responsable y/o el uso que se les ha dado, en los términos y plazos legales.
4.15. Reclamo
Solicitud del titular relacionada con la corrección, actualización, supresión, revocatoria o el presunto incumplimiento del régimen de protección de datos, con trámite y términos legales.
4.16. Incidente de seguridad de la información
Evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de los datos personales (pérdida, acceso no autorizado, fuga, alteración, destrucción, ransomware, error humano, envío a destinatario equivocado, exposición en web, etc.). Debe registrarse y gestionarse conforme al procedimiento interno, y reportarse a la autoridad cuando corresponda.
4.17. Transferencia de datos personales
Envío de datos personales desde la Red a un tercero que actúa como responsable, ubicado dentro o fuera de Colombia, para que realice tratamiento por cuenta propia y con sus finalidades (debe existir base legal, garantías y, cuando aplique, requisitos de transferencias internacionales).
4.18. Transmisión de datos personales
Comunicación de datos personales desde la Red a un encargado, ubicado dentro o fuera de Colombia, para que trate los datos por cuenta de la Red y conforme a sus instrucciones (requiere contrato de transmisión u otro instrumento equivalente).
4.19. Circulación restringida
Principio según el cual los datos personales solo pueden ser accesibles y circulados por personas autorizadas y en el marco de finalidades legítimas, evitando exposición innecesaria (incluye controles por roles, confidencialidad, necesidad de saber).
4.20. Seudonimización (pseudonimización)
Tratamiento por el cual los datos ya no pueden atribuirse a un titular sin usar información adicional (tabla de correspondencias), la cual debe mantenerse separada, bajo custodia y con acceso restringido. No equivale a anonimización irreversible.
4.21. Anonimización
Proceso técnico y organizacional orientado a eliminar o transformar datos personales de forma que el titular no sea identificable por medios razonables, reduciendo significativamente el riesgo de reidentificación. Se aplica especialmente a informes públicos, rendición de cuentas, datasets o piezas de comunicación.
4.22. Disociación
Técnica o conjunto de técnicas para separar la información del titular de los datos, de modo que no pueda asociarse directa o indirectamente sin información adicional, o para impedir identificación en el producto final (p. ej. supresión de identificadores, generalización). En esta política, disociación se entiende como parte del estándar de anonimización para divulgación.
4.23. Riesgo de reidentificación

Probabilidad de que un tercero pueda inferir o reconstruir la identidad del titular a partir de información publicada (combinación de variables, contexto territorial, notoriedad del caso, fuentes abiertas). Determina el nivel de anonimización exigido.

4.24. Violación de datos personales (data breach)

Cualquier evento de seguridad que ocasione destrucción, pérdida, alteración, divulgación no autorizada o acceso no autorizado a datos personales transmitidos, conservados o tratados por la Red.

5. Roles y gobernanza

5.1. Responsable del Tratamiento (modelo Red)

La Red, a través de sus veedurías integrantes, actuará como Responsable del Tratamiento respecto de los datos personales que recolecte, administre y use en el marco de sus funciones. Bajo este modelo:

a) Responsabilidad por veeduría (descentralizada)

- Cada veeduría que recolecte datos personales y determine sus finalidades y medios de tratamiento actúa como Responsable de las bases de datos bajo su administración.
- Cada veeduría deberá:
    1. Identificar y mantener inventario de bases de datos, canales y flujos.
    2. Establecer finalidades y bases jurídicas del tratamiento.
    3. Asegurar autorizaciones y/o habilitaciones legales cuando aplique.
    4. Implementar medidas de seguridad (administrativas, técnicas y humanas) acordes al riesgo.
    5. Definir responsables internos por proceso (misional, PQRS, comunicaciones, TI, talento humano, archivo).
    6. Atender consultas y reclamos de titulares dentro de términos legales.
    7. Gestionar incidentes, incluyendo registro, respuesta, reporte y medidas correctivas.

b) Repositorios unificados o plataformas comunes (responsabilidad conjunta o responsable principal)

Cuando exista una plataforma unificada, repositorio nacional/regional o base consolidada operada por la Red (o por una instancia coordinadora), se definirá explícitamente, mediante acto interno, una de las siguientes modalidades:

- Responsabilidad conjunta: cuando dos o más veedurías definan conjuntamente finalidades y medios del tratamiento (p. ej., repositorio federado).
- Responsable principal + corresponsables: cuando una instancia coordinadora administre la plataforma y defina estándares y finalidades marco, y las veedurías aporten y consulten información bajo reglas comunes.

En ambos casos, el acto interno deberá fijar como mínimo:

1. La distribución de obligaciones (atención de derechos, seguridad, registros, incidentes).
2. Las reglas de acceso (roles, necesidad de saber, trazabilidad).
3. Estándares de anonimización, publicación y circulación restringida.
4. Los procedimientos de transmisión/transferencia con terceros.
5. Custodia y gobierno de llaves de seudonimización cuando aplique.

Nota operativa clave: si el repositorio unificado es operado por un proveedor tecnológico externo, este actuará como Encargado del Tratamiento y deberá existir contrato/instrumento de transmisión con obligaciones de seguridad, confidencialidad, subencargados y retorno/supresión.

5.2. Encargado del Tratamiento (proveedores y terceros operativos)

Son Encargados todas las personas naturales o jurídicas que, por contrato o relación funcional, traten datos personales por cuenta de la Red (o de una veeduría responsable), conforme a instrucciones documentadas.

Obligaciones mínimas del Encargado (estándar Red):

- Tratar datos solo conforme a instrucciones del responsable.
- Implementar medidas de seguridad acordes al riesgo.
- Mantener confidencialidad del personal con acceso.
- Reportar incidentes sin dilación al responsable/OPD.
- No subcontratar sin autorización y condiciones equivalentes.
- Permitir auditorías y evidenciar cumplimiento.
- Devolver o suprimir datos al terminar el contrato, salvo retención legal.

5.3. Oficial de Protección de Datos (OPD)

La Red designará un Oficial de Protección de Datos (o su equivalente institucional) como responsable de coordinar y verificar el cumplimiento de esta política y del régimen aplicable, sin perjuicio de las responsabilidades propias de cada veeduría.

Funciones mínimas del OPD:

1. Vigilancia y cumplimiento: verificar la aplicación de la política, emitir lineamientos internos y coordinar planes de mejora.
2. Atención de titulares: coordinar y/o supervisar la atención de consultas y reclamos, y asegurar trazabilidad de respuestas.
3. Gestión de incidentes: recibir reportes, activar respuesta, mantener el registro de incidentes, coordinar análisis de causa raíz y plan de acción.
4. Anonimización y publicaciones: validar o co-validar estándares y procedimientos de anonimización para informes públicos y rendición de cuentas.
5. Auditoría y control: programar auditorías internas, revisiones de cumplimiento y pruebas de reidentificación cuando se publiquen datos.
6. Capacitación: diseñar y coordinar formación periódica en protección de datos, reserva de identidad y anonimización.
7. Asesoría interna: orientar sobre bases legales, minimización, retención y divulgación segura.
8. Articulación con TI y Archivo: asegurar que controles de acceso, backups, logs y retención documental sean coherentes con privacidad y seguridad.
9. Gestión documental de privacidad: custodiar versiones de la política, avisos de privacidad, cláusulas tipo, formatos de autorización y matrices.

Recomendación estructural: en la Red, el OPD puede estar apoyado por enlaces de privacidad en cada veeduría (punto focal), responsables de ejecutar lineamientos y reportar novedades.

5.4. Comité de Seguridad y Privacidad de la Información

La Red contará con un Comité de Seguridad y Privacidad de la Información (o instancia equivalente), como órgano de coordinación y decisión técnica sobre riesgos, controles, publicación y gobierno de datos.

Integración

- Coordinación de la Red (o quien haga sus veces).
- OPD (secretaría técnica).
- Líder de TI / Seguridad digital.
- Líder misional (denuncias/PQRS/seguimiento).
- Líder de archivo/gestión documental.
- Comunicaciones (por impacto en publicaciones).
- Jurídica (cuando aplique).

Funciones mínimas del Comité:

1. Aprobar lineamientos de seguridad, acceso y clasificación de información.
2. Aprobar el estándar de anonimización/disociación y sus niveles (bajo/medio/alto) para publicaciones e informes.
3. Definir criterios de reserva de identidad en denuncias y protección de testigos/denunciantes.
4. Evaluar incidentes relevantes y aprobar medidas correctivas y preventivas.
5. Aprobar el plan anual de capacitación y auditoría.
6. Revisar y recomendar actualizaciones de la política ante cambios normativos o de riesgo.

5.5. Responsables por proceso (líneas de ejecución)

Para asegurar implementación real, cada veeduría definirá responsables funcionales por procesos (mínimo):

- Misional – Denuncias/PQRS: recolección, reserva, minimización, custodia de evidencias.
- TI y seguridad: accesos, respaldos, cifrado, gestión de vulnerabilidades.
- Archivo y gestión documental: retención, conservación, eliminación segura, control de préstamos.
- Comunicaciones: control de publicación, anonimización previa, gestión de imagen/voz.
- Talento humano y contratación: cláusulas de confidencialidad, contratos de transmisión, control de accesos a personal saliente.

6. Roles y gobernanza

6.1. Responsable del Tratamiento (modelo Red)

La Red, a través de sus veedurías integrantes, actuará como Responsable del Tratamiento respecto de los datos personales que recolecte, administre y utilice en el marco de sus funciones.

a) Responsabilidad por veeduría (descentralizada)

- Cada veeduría que recolecte datos personales y determine finalidades y medios del tratamiento actúa como Responsable de las bases de datos bajo su administración.
- En consecuencia, cada veeduría deberá, como mínimo:
    1. Mantener inventario de bases de datos, canales y flujos de información.
    2. Definir finalidades, términos de conservación y controles de acceso.
    3. Asegurar autorizaciones cuando sean exigibles y soportar habilitaciones legales cuando aplique.

4. Implementar medidas de seguridad administrativas, técnicas y humanas, acordes con el riesgo.
5. Garantizar la atención de consultas y reclamos de titulares dentro de los términos legales.
6. Gestionar incidentes de seguridad, incluyendo registro, respuesta, corrección y reporte cuando corresponda.
7. Asegurar la anonimización/disociación en productos públicos y divulgaciones, conforme al procedimiento interno.

b) Repositorios unificados (nacional o regional) y corresponsabilidad
Cuando exista un repositorio unificado, plataforma compartida o base consolidada operada por una instancia de coordinación de la Red, se definirá mediante acto interno una de estas modalidades:

- Responsabilidad conjunta (corresponsables): cuando dos o más veedurías definan conjuntamente finalidades y medios del tratamiento.
- Responsable principal y corresponsables: cuando una instancia coordinadora administre la plataforma y establezca estándares, y las veedurías aporten/consulten información bajo reglas comunes.

En cualquier modalidad, el acto interno deberá precisar como mínimo:

1. Distribución de obligaciones (atención de titulares, seguridad, publicaciones, incidentes).
2. Reglas de acceso y trazabilidad (roles, "necesidad de saber", auditoría).
3. Estándares y niveles de anonimización/disociación para divulgación.
4. Procedimientos de transmisión/transferencia y control de terceros.
5. Custodia de llaves de seudonimización, cuando se utilicen.

6.2. Encargado del Tratamiento (proveedores y terceros operativos)
Son Encargados del Tratamiento las personas naturales o jurídicas que, por contrato o instrumento equivalente, tratan datos personales por cuenta de la Red o de una veeduría Responsable, conforme a instrucciones documentadas (p. ej. proveedores TI, nube, PQRS, digitalización, archivo, mensajería, productoras audiovisuales o agencias de comunicación).
Obligaciones mínimas del Encargado:

1. Tratar los datos únicamente conforme a instrucciones del Responsable.
2. Adoptar medidas de seguridad acordes con el riesgo y la sensibilidad.
3. Garantizar confidencialidad del personal con acceso y controlar subencargados.
4. Reportar incidentes de forma inmediata al Responsable y al OPD.
5. Permitir auditorías y aportar evidencia de cumplimiento.
6. Devolver o suprimir datos al terminar el servicio, salvo obligación legal de conservación.

6.3. Oficial de Protección de Datos (OPD)
La Red designará un Oficial de Protección de Datos (o instancia equivalente) para coordinar y verificar la implementación de esta política, sin perjuicio de las responsabilidades propias de cada veeduría.
Funciones mínimas del OPD:

1. Vigilar el cumplimiento de la política y emitir lineamientos internos.
2. Coordinar la atención de titulares (consultas y reclamos) y su trazabilidad.

3. Liderar la gestión de incidentes: recepción, registro, análisis, plan de acción y seguimiento.
4. Coordinar auditorías internas y revisiones periódicas de cumplimiento.
5. Validar (o co-validar) estándares de anonimización/disociación para publicaciones.
6. Coordinar planes de capacitación y cultura de protección de datos.
7. Articular acciones con TI, Gestión Documental y Comunicaciones para controles de acceso, retención y divulgación segura.

Enlaces de privacidad (recomendado): cada veeduría podrá designar un punto focal que apoye al OPD en ejecución territorial, reporte de incidentes y control de publicaciones.

6.4. Comité de Seguridad y Privacidad de la Información

La Red contará con un Comité de Seguridad y Privacidad de la Información como instancia de coordinación técnica y decisión sobre riesgos, controles, anonimización y divulgación.

Integración mínima sugerida:

- Coordinación de la Red (o quien haga sus veces).
- OPD (secretaría técnica).
- Líder de TI/seguridad digital.
- Líder misional (denuncias/PQRS).
- Líder de Archivo/Gestión Documental.
- Comunicaciones.
- Jurídica (cuando aplique).

Funciones mínimas:

1. Definir y aprobar lineamientos de seguridad, acceso, clasificación y circulación restringida.
2. Aprobar estándares y niveles de anonimización/disociación para informes, transparencia y piezas públicas.
3. Establecer criterios de reserva de identidad y protección reforzada en denuncias.
4. Conocer incidentes relevantes y aprobar medidas correctivas y preventivas.
5. Aprobar el plan anual de capacitación, auditoría y mejora continua.
6. Recomendar actualizaciones de la política ante cambios normativos o de riesgo.

6.5. Responsables por proceso (líneas de ejecución)

Para asegurar implementación real, cada veeduría definirá responsables funcionales por procesos (mínimo), quienes deberán operar controles, evidencias y reportes:

a) Misional – Denuncias/PQRS

- Recolección legítima y minimizada de datos.
- Aplicación de reserva y circulación restringida.
- Custodia de evidencias, control de acceso por roles y trazabilidad.
- Activación del procedimiento de anonimización para informes/casos públicos.

b) TI y seguridad

- Gestión de accesos (altas/bajas), contraseñas y autenticación reforzada cuando aplique.
- Respaldos, cifrado, continuidad, gestión de vulnerabilidades.
- Monitoreo, logs, gestión de incidentes técnicos y recuperación.

c) Archivo y gestión documental

- Retención, conservación, transferencias documentales y eliminación segura.
- Control de préstamo, reproducción, digitalización y custodia.

- Aplicación de reglas de reserva y supresión conforme a tiempos definidos.

d) Comunicaciones

- Control previo de publicación (checklist de datos personales).
- Anonimización/disociación obligatoria en piezas públicas.
- Gestión segura de imagen/voz y metadatos (foto/video/audio).
- Archivo de soportes de anonimización y de autorizaciones cuando aplique.

e) Talento humano y contratación

- Cláusulas de confidencialidad y obligaciones de tratamiento en contratos.
- Instrumentos de transmisión con encargados y control de subcontratación.
- Gestión de accesos de personal entrante/saliente y devolución de activos.

6.6. Matriz RACI y evidencias mínimas (recomendado)

Para evitar vacíos, la Red adoptará una matriz RACI (Responsable–Aprobador–Consultado–Informado) y definirá evidencias mínimas obligatorias, como:

- Inventario de bases y flujos;
- Registro de autorizaciones/habilitaciones;
- Registro de incidentes y planes de acción;
- Matrices de anonimización y actas de validación de publicación;
- Contratos de transmisión y evaluaciones de proveedores.

7. Principios rectores del tratamiento

7.1. Observancia del marco legal y enfoque de responsabilidad demostrada

La Red realizará el tratamiento de datos personales en estricto cumplimiento del régimen colombiano de protección de datos personales y demás normas aplicables. En desarrollo del principio de responsabilidad demostrada (accountability), la Red implementará medidas jurídicas, técnicas y organizacionales para acreditar el cumplimiento de esta política, incluyendo evidencia documental de: finalidades, bases jurídicas/autoridades, autorizaciones cuando aplique, gestión de riesgos, controles de acceso, anonimización, atención de titulares y gestión de incidentes.

7.2. Principio de legalidad

El tratamiento de datos personales es una actividad reglada y solo podrá realizarse conforme a la Constitución, la ley y la normativa aplicable. La Red no recolectará ni tratará datos por medios fraudulentos, engañosos o no autorizados, ni para finalidades prohibidas.

7.3. Principio de finalidad

Los datos personales serán recolectados y tratados para fines específicos, explícitos, legítimos y previamente informados al titular o amparados en habilitación legal. Está prohibido el tratamiento para finalidades incompatibles con aquellas informadas o legalmente definidas, salvo que exista una nueva base jurídica que lo permita.

7.4. Principio de libertad

El tratamiento solo podrá ejercerse con el consentimiento previo, expreso e informado del titular, cuando sea exigible, o con fundamento en habilitación legal. Está prohibida la obtención de datos mediante coacción, condicionamientos injustificados o prácticas que afecten la autodeterminación informativa.

7.5. Principio de veracidad o calidad

La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. La Red adoptará medidas razonables para su actualización y corrección, y se abstendrá de tratar datos parciales, fraccionados o que induzcan a error cuando ello afecte derechos o decisiones.

7.6. Principio de transparencia

La Red garantizará el derecho del titular a obtener información clara, suficiente y oportuna sobre la existencia de datos que le conciernan, el uso dado a los mismos, las finalidades del tratamiento y los canales para ejercer sus derechos, salvo las limitaciones legales aplicables (por ejemplo, reserva legal, debido proceso o protección de denunciantes y testigos).

7.7. Principio de acceso y circulación restringida

El tratamiento se sujetará a límites derivados de la naturaleza del dato, las finalidades autorizadas y la normativa aplicable. En consecuencia:

- El acceso estará regido por el criterio de "necesidad de saber" y por roles definidos.
- La información no será accesible al público ni divulgada sin habilitación legal, autorización o procedimiento de anonimización cuando corresponda.
- En contextos de denuncias, víctimas, testigos, denunciantes o NNA, se aplicarán medidas reforzadas de restricción y anonimización.

7.8. Principio de seguridad

La Red adoptará medidas de seguridad técnicas, humanas y administrativas razonables y proporcionales al riesgo, para evitar adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Esto incluye, como mínimo: control de accesos, trazabilidad, copias de seguridad, gestión de vulnerabilidades, protección de dispositivos y gestión de incidentes.

7.9. Principio de confidencialidad

Todas las personas que intervengan en el tratamiento de datos personales están obligadas a garantizar la reserva de la información, aun después de finalizar su relación con la Red. La confidencialidad será exigible mediante compromisos, cláusulas contractuales y controles disciplinarios o legales cuando aplique.

7.10. Principio de minimización y proporcionalidad (regla operativa)

La Red recolectará y tratará únicamente los datos estrictamente necesarios para cumplir la finalidad. Se evitará el exceso de información, la duplicidad de recolección y la conservación indefinida sin justificación. La minimización será obligatoria en denuncias y PQRS, especialmente respecto de datos sensibles.

7.11. Principio de temporalidad o limitación del almacenamiento (regla operativa)

Los datos serán conservados por el tiempo estrictamente necesario para cumplir la finalidad y las obligaciones legales/archivísticas aplicables, y posteriormente serán suprimidos o anonimizados conforme al procedimiento interno de retención y eliminación segura.

7.12. Principio de privacidad desde el diseño y por defecto (regla operativa)

En el diseño o adopción de canales, sistemas, formatos y procedimientos, la Red incorporará controles de privacidad desde la planeación (privacy by design) y configuraciones de máxima protección por defecto (privacy by default), incluyendo: parámetros restrictivos de acceso, registros de auditoría, anonimización en reportes, y limitación de publicación de datos.

7.13. Principio de no discriminación y enfoque diferencial (regla operativa)

La Red evitará cualquier tratamiento que genere discriminación o estigmatización. En casos que involucren datos sensibles o poblaciones con especial protección (NNA, víctimas, personas en riesgo), se aplicará un estándar reforzado de anonimización y circulación restringida, procurando prevenir revictimización y represalias.

8. Finalidades del tratamiento (catálogo base)

8.1. Regla general de determinación de finalidades

La Red tratará datos personales únicamente para finalidades legítimas, específicas, explícitas y verificables, informadas al Titular cuando sea exigible, o sustentadas en habilitación legal. Las finalidades deberán estar asociadas a funciones misionales y de apoyo, evitando usos incompatibles o excesivos.

8.2. Finalidades misionales (control social, veeduría y seguimiento)

La Red podrá tratar datos personales para:

8.2.1. Recepción, radicación y gestión de denuncias, quejas y reportes

- Recibir información ciudadana y evidencias (documentos, imágenes, audios, videos).
- Validar requisitos mínimos de radicación y trazabilidad.
- Clasificar y priorizar casos conforme a criterios internos de riesgo e impacto.

8.2.2. Verificación, análisis y seguimiento de casos

- Contrastar información y realizar verificaciones documentales y de contexto.
- Elaborar conceptos, reportes técnicos y matrices de seguimiento.
- Gestionar actuaciones internas para impulsar control social o requerimientos institucionales.

8.2.3. Articulación interinstitucional y remisiones

- Remitir actuaciones o hallazgos a autoridades competentes (organismos de control, autoridades administrativas o judiciales), conforme a la ley y a reglas de reserva.
- Atender requerimientos oficiales y solicitudes de información con soporte legal.

8.2.4. Protección de denunciantes, testigos y personas en riesgo

- Implementar mecanismos internos de reserva de identidad.
- Aplicar medidas de anonimización/disociación y circulación restringida.
- Gestionar alertas o escalamiento interno cuando existan riesgos de represalia.

8.2.5. Gestión de evidencias y custodia

- Administrar repositorios de evidencias con controles de acceso, trazabilidad, cadena de custodia cuando aplique y medidas de seguridad reforzadas.

8.3. Finalidades de atención ciudadana y relacionamiento (canales)

La Red podrá tratar datos personales para:

8.3.1. Atención de PQRS y derechos de petición

- Recibir, tramitar y responder peticiones, quejas, reclamos, sugerencias y solicitudes.
- Realizar notificaciones, comunicaciones y seguimiento del estado del trámite.

8.3.2. Contacto con la ciudadanía y gestión de comunicaciones funcionales

- Contactar al Titular para aclaraciones, ampliaciones, validaciones o entrega de respuesta.
- Gestionar agendas, citaciones y coordinación de reuniones relacionadas con casos o actuaciones.

8.4. Finalidades de transparencia, rendición de cuentas y divulgación (con anonimización)

La Red podrá tratar datos personales para:

8.4.1. Rendición de cuentas e informes de gestión

- Elaborar informes institucionales y estadísticos sobre resultados, avances y tendencias.
- Publicar información agregada o anonimizada para evitar reidentificación.

8.4.2. Producción de contenidos institucionales

- Desarrollar boletines, comunicados, piezas de comunicación y material pedagógico.
- Documentar experiencias y resultados, aplicando anonimización obligatoria cuando existan casos, denuncias o información sensible.

8.4.3. Transparencia y acceso a información pública

- Atender solicitudes de información pública, aplicando las reservas legales y la protección de datos personales mediante supresión o anonimización.

Regla de oro: la divulgación de casos reales solo procederá si (i) existe habilitación legal o autorización cuando aplique, (ii) no se vulneran reservas o debido proceso, y (iii) se aplica anonimización/disociación y control de reidentificación.

8.5. Finalidades administrativas y de gestión institucional

La Red podrá tratar datos personales para:

8.5.1. Gestión del talento humano

- Vinculación, administración, bienestar, formación, control de acceso y seguridad interna.
- Gestión disciplinaria interna cuando corresponda y con reserva.

8.5.2. Gestión contractual y de proveedores

- Selección, contratación, supervisión/interventoría, pagos y evaluación de desempeño de contratistas y proveedores.
- Gestión de habilitaciones, cumplimiento y control de acceso a información.

8.5.3. Gestión financiera y contable (si aplica)

- Cumplimiento de obligaciones contables, fiscales y de control interno, con minimización de datos.

8.6. Finalidades tecnológicas, seguridad y continuidad

La Red podrá tratar datos personales para:

8.6.1. Administración de plataformas, sistemas y soporte

- Operación de herramientas de radicación, PQRS, gestión documental y repositorios.
- Mesa de ayuda, mantenimiento, auditoría técnica y control de cambios.

8.6.2. Seguridad de la información y ciberseguridad

- Gestión de accesos, autenticación, trazabilidad, monitoreo, logs y prevención de fraude.
- Prevención, detección y respuesta a incidentes de seguridad.

8.6.3. Continuidad del negocio y recuperación

- Respaldos, recuperación ante desastres, contingencia y resiliencia operacional.

8.7. Finalidades de cumplimiento legal, defensa jurídica y requerimientos de autoridad

La Red podrá tratar datos personales para:

8.7.1. Cumplimiento de obligaciones legales y regulatorias

- Responder a requerimientos de autoridades administrativas, judiciales u organismos de control.
- Cumplir con deberes de archivo, conservación, reporte y control.

8.7.2. Defensa jurídica y gestión de riesgos legales

- Atención y trámite de acciones judiciales, conciliaciones, reclamaciones, auditorías o investigaciones relacionadas con la Red.

8.8. Finalidades de investigación, análisis y mejora (con salvaguardas)

La Red podrá tratar datos personales para:

8.8.1. Analítica institucional y mejora de procesos

- Analizar tiempos de respuesta, calidad del servicio, riesgos recurrentes y necesidades territoriales.

8.8.2. Estudios e investigaciones (si aplica)

- Elaborar estudios internos o con aliados académicos, siempre bajo principios de minimización, anonimización y acuerdos de confidencialidad, priorizando datos agregados o disociados.

8.9. Restricciones generales aplicables a todas las finalidades

- Prohibición de lucro/comercialización: la Red no comercializa datos personales ni realiza tratamiento con fines de mercadeo sin autorización específica.
- No se tratarán datos sensibles salvo que exista justificación, base legal o autorización explícita, y medidas reforzadas.
- No publicación de identidad de denunciantes, testigos, víctimas o NNA en productos públicos.
- Minimización obligatoria: se recolecta solo lo necesario y se conserva lo estrictamente indispensable.

8.10. Actualización del catálogo de finalidades

El presente catálogo podrá actualizarse por acto interno cuando cambien funciones, procesos o sistemas, garantizando: (i) publicidad de la actualización, (ii) ajuste del aviso de privacidad, (iii) evaluación de riesgos y (iv) actualización de estándares de anonimización.

9.2. Datos sensibles

9.2.1. Regla de restricción

Los datos sensibles se tratan de forma excepcional. La Red solo los recolectará y tratará cuando sea estrictamente necesario para una finalidad legítima y exista una base habilitante válida.

9.2.2. Condiciones habilitantes (cuándo se pueden tratar)

El tratamiento de datos sensibles solo procederá cuando concurra al menos una de estas condiciones:

a) Autorización explícita del titular

- Debe ser expresa, previa, informada y verificable.
- Debe indicar con claridad la finalidad específica y el carácter sensible del dato.

b) Habilitación legal aplicable

Cuando la autorización no sea exigible por existir fundamento legal suficiente, especialmente en contextos misionales de interés público, protección de derechos, cumplimiento de funciones públicas o atención de requerimientos de autoridad, con aplicación estricta de medidas reforzadas.

En todos los casos, se deberá documentar la base habilitante (autorización u habilitación legal) y la justificación de necesidad y proporcionalidad.

9.2.3. Prohibiciones y límites

- Queda prohibido condicionar la atención de una denuncia/PQRS a la entrega de datos sensibles que no sean necesarios.
- Está prohibida la divulgación de datos sensibles en productos públicos, salvo que: (i) exista autorización expresa para esa divulgación específica o (ii) exista una obligación legal clara, y siempre aplicando evaluación de riesgo y medidas de minimización.

9.2.4. Medidas reforzadas obligatorias para datos sensibles

Cuando se traten datos sensibles, la Red aplicará, como mínimo:

1. Acceso restringido por roles (“necesidad de saber”).
2. Registro de accesos y trazabilidad (quién accede, cuándo y para qué).
3. Custodia reforzada de evidencias (repositorios segregados cuando aplique).
4. Cifrado o medidas equivalentes de protección en almacenamiento y transmisión, según criticidad.
5. Anonimización/disociación obligatoria en informes y divulgación externa.
6. Acuerdos de confidencialidad para personal y terceros con acceso.

9.3. Datos personales de niños, niñas y adolescentes (NNA)

9.3.1. Regla general

El tratamiento de datos de NNA se presume restringido y exige un estándar reforzado, atendiendo el interés superior del menor y la prevalencia de sus derechos.

9.3.2. Condiciones mínimas para el tratamiento

La Red solo tratará datos de NNA cuando:

1. Sea necesario y proporcional para una finalidad legítima (p. ej., protección de derechos, activación de rutas, atención de requerimientos de autoridad).
2. Se adopten garantías reforzadas de reserva, seguridad y circulación restringida.
3. Se verifique la legitimación: representante legal o autoridad competente cuando aplique.
4. Se evite la recolección de datos sensibles de NNA salvo estricta necesidad y con controles máximos.

9.3.3. Publicación y divulgación (regla estricta)

- Se prohíbe publicar información que permita identificar directa o indirectamente a NNA en informes, boletines, piezas de comunicación, contenidos web o redes sociales.
- Cualquier uso en rendición de cuentas será exclusivamente agregado o anonimizado con control de reidentificación.

9.4. Denuncias y procesos (administrativos, disciplinarios y/o judiciales): reglas por defecto

9.4.1. Reserva de identidad y protección de personas

En denuncias y procesos, la Red aplicará por defecto:

- Reserva de identidad de denunciantes, testigos, víctimas e informantes en todo producto de divulgación o comunicación, salvo:
    1. orden judicial o requerimiento legal expreso y competente, o
    2. habilitación legal clara que exija su identificación, con evaluación de riesgo y medidas de protección.

9.4.2. Anonimización obligatoria para divulgación y transparencia

Será obligatoria la anonimización/disociación (y, cuando aplique, agregación) en:

- Informes públicos y rendición de cuentas con casos.
- Comunicados, boletines, notas de prensa y piezas pedagógicas.
- Publicaciones web, redes sociales y repositorios abiertos.
- Datasets o entregables de transparencia activa.

9.4.3. Circulación restringida y control de acceso en expedientes

- Los expedientes y evidencias se manejarán con acceso restringido por roles, con trazabilidad y custodia.

- Se prohíbe el envío informal de piezas del expediente por canales no autorizados o sin cifrado cuando el riesgo lo amerite.
- La entrega de copias a terceros se hará únicamente por canales institucionales y con verificación de legitimación y finalidad.

9.5. Evaluación de riesgo y test de reidentificación (obligatorio antes de publicar)
Antes de publicar o divulgar información derivada de denuncias o procesos que involucre datos sensibles o NNA, se realizará:

1. Clasificación de sensibilidad (bajo/medio/alto).
2. Identificación de identificadores directos y cuasi-identificadores.
3. Selección de técnica (supresión, generalización, seudonimización, agregación).
4. Prueba razonable de reidentificación (especialmente en territorios pequeños).
5. Aprobación conforme al modelo de gobernanza (Comunicaciones + OPD/Comité, según aplique).

9.6. Registro, trazabilidad y evidencia de cumplimiento
Toda actuación relacionada con datos sensibles o de NNA deberá dejar evidencia mínima:

- Justificación de necesidad y proporcionalidad.
- Base habilitante (autorización o habilitación legal).
- Matriz de anonimización (si hay divulgación).
- Registro de accesos (cuando aplique).
- Registro de incidentes, si ocurrieran, y plan de acción.

10. Autorización y prueba (garantías reforzadas) – ampliado y detallado

Nota de coherencia de numeración: en tu estructura actual, este capítulo puede quedar como Numeral 10, después del 9. Tratamiento de datos sensibles y de NNA. Si en tu índice definitivo "Autorización y prueba" debe ser 8, lo renumero sin problema; aquí lo dejo como 10 para que no se cruce con lo ya trabajado.
10.1. Regla general de autorización (cuándo se solicita)
La Red solicitará autorización previa, expresa, informada y verificable del titular para el tratamiento de sus datos personales cuando sea exigible, antes o al momento de la recolección, indicando como mínimo:

1. Identidad del Responsable del Tratamiento y canales de contacto.
2. Finalidades específicas del tratamiento.
3. Derechos del titular y cómo ejercerlos (consultas, reclamos, supresión, revocatoria).
4. Carácter facultativo u obligatorio de suministrar datos (y qué ocurre si no se entregan).
5. Si se recolectarán datos sensibles o de NNA, indicando el carácter sensible y el estándar reforzado de protección.
6. Posibles destinatarios (encargados/proveedores) y existencia de transmisión/transferencia, si aplica.
7. Tiempo de conservación o criterios para determinarlo.
8. Referencia y acceso a la Política de Tratamiento y al Procedimiento de Anonimización.

10.2. Requisitos de validez y garantías de protección de la autorización (estándar de prueba)
Para que la autorización sea válida y defendible, la Red garantizará:
10.2.1. Claridad y comprensibilidad

- Lenguaje claro, no ambiguo, evitando términos técnicos no explicados.
- Finalidades concretas (no genéricas del tipo "para fines institucionales" sin precisión).

10.2.2. Especificidad (finalidades delimitadas)

- La autorización debe corresponder a finalidades definidas en el catálogo del numeral 8.
- Si surge una finalidad nueva o incompatible, se deberá obtener nueva autorización o soportar habilitación legal.

10.2.3. Libertad (no condicionamiento indebido)

- La Red no condicionará indebidamente la atención o el trámite de una denuncia/PQRS a la entrega de datos no necesarios.
- En casos misionales, se aplicará minimización: se solicitarán solo los datos indispensables para contacto y trazabilidad.

10.2.4. Evidenciabilidad (capacidad de demostración)

- Toda autorización debe quedar respaldada por evidencia verificable y recuperable (trazabilidad).
- Las autorizaciones se administrarán bajo un esquema de control documental (fecha, canal, versión del texto informado).

10.2.5. Especialidad para datos sensibles

- Cuando se traten datos sensibles, la autorización deberá ser explícita y distinguir el dato sensible y su finalidad.
- Debe incluir advertencia sobre el carácter facultativo de responder, y el estándar reforzado de seguridad y acceso restringido.

10.2.6. NNA (legitimación y estándar reforzado)

- En datos de NNA, se verificará la legitimación (representante legal o autoridad competente cuando aplique) y se aplicará interés superior.
- En ningún caso se divulgará información identificable de NNA; cualquier uso público será agregado o anonimizado.

10.3. Canales y formas aceptadas de autorización (con trazabilidad)

La Red podrá obtener autorización, cuando sea exigible, por cualquiera de los siguientes medios, siempre que sean trazables:

10.3.1. Escrita (física o digital)

- Formatos firmados, formularios web con casilla de aceptación y registro de auditoría, firma electrónica o digital cuando aplique.

10.3.2. Verbal (con soporte)

- Autorización verbal mediante llamada o atención presencial solo si se conserva soporte verificable: grabación, acta firmada, registro de atención con confirmación del texto informado.

10.3.3. Conducta inequívoca (cuando sea jurídicamente admisible)

- Acciones claras del titular que evidencien consentimiento, con soporte (p. ej., envío voluntario de información a un canal que informa previamente finalidades y política).
- En todo caso, la Red documentará el texto informado al momento de la recolección y el registro de la interacción.

10.4. Prueba del cumplimiento (qué evidencia debe conservar la Red)

La Red conservará evidencia suficiente de:

10.4.1. La autorización (cuando sea exigible)

Como mínimo:

- Fecha y hora.
- Canal de recolección (web, correo, presencial, teléfono, WhatsApp institucional).
- Identificación del titular (o código interno si aplica).
- Texto/versión del aviso de privacidad o cláusula aceptada.
- Evidencia del acto de aceptación (firma, check, grabación, acta, registro del sistema).
- Identificación del funcionario/operador que recibió la autorización.

10.4.2. La causal legal habilitante (cuando no se requiera autorización)
En los eventos en que el tratamiento se funde en habilitación legal (función pública, deber legal, requerimiento de autoridad, protección de derechos, defensa jurídica, etc.), se deberá conservar:

- Justificación de necesidad y proporcionalidad.
- Identificación del proceso misional asociado.
- Referencia a la norma o fundamento aplicable (o acto/requerimiento).
- Alcance del tratamiento (qué datos, para qué, por cuánto tiempo, quién accede).
- Medidas de seguridad aplicadas (acceso, reserva, anonimización si hay divulgación).

10.5. Garantías de protección de la prueba (seguridad y custodia)
Para proteger la evidencia de autorización/habilitación y evitar alteraciones o accesos indebidos, la Red implementará:

10.5.1. Custodia y acceso restringido

- Las evidencias se almacenarán en repositorios institucionales definidos (no en dispositivos personales).
- Acceso limitado por rol: OPD, líderes de proceso, archivo y jurídico según corresponda.
- Prohibición de reenvíos por canales no autorizados.

10.5.2. Integridad y trazabilidad

- Control de versiones del texto de autorización/aviso de privacidad.
- Registro de auditoría (logs) sobre creación, modificación y consulta de evidencias digitales.
- Cuando aplique: sellos de tiempo, hash o mecanismos equivalentes para evidenciar integridad.

10.5.3. Confidencialidad reforzada

- Cifrado o protección equivalente para repositorios con evidencias que incluyan datos sensibles, NNA, denunciantes o testigos.
- Compromisos de confidencialidad y control contractual para proveedores encargados.

10.5.4. Retención y conservación

- La prueba se conservará durante el tiempo necesario para:
  (i) acreditar licitud del tratamiento,
  (ii) responder reclamaciones o investigaciones, y
  (iii) cumplir obligaciones archivísticas y de control.
- Vencidos los términos aplicables, se aplicará eliminación segura o anonimización, según proceda.

10.5.5. Continuidad y contingencia

- Copias de seguridad bajo controles de acceso.
- Procedimientos de recuperación ante pérdida o incidente.
- Pruebas periódicas de restauración cuando aplique.

10.6. Revocatoria y actualización de autorizaciones (control de cambios)
Cuando el titular revoque autorización o solicite supresión, la Red:

- Verificará identidad y legitimación.
- Evaluará si existe deber legal/contractual de conservación.
- Ejecutará la decisión (supresión, bloqueo, anonimización) y dejará evidencia del trámite.
- Actualizará sistemas y repositorios donde se replique la información, dentro de un plazo razonable.

10.7. Anexos recomendados

Para blindar "prueba y autorización", se recomienda anexar al documento:

- Anexo A: Modelo de "Aviso de privacidad" para PQRS/denuncias (web y presencial).
- Anexo B: Formato de autorización explícita para datos sensibles.
- Anexo C: Formato/bitácora de recolección verbal (llamada/atención presencial).
- Anexo D: Matriz "finalidad–dato–base habilitante–retención–nivel de anonimización".
- Anexo E: Checklist de control de evidencias (custodia, logs, cifrado, backups).

11. Derechos de los titulares y procedimientos

11.1. Derechos mínimos de los titulares (habeas data)

La Red reconoce y garantiza a los titulares, como mínimo, los siguientes derechos:

11.1.1. Conocer (acceder) a sus datos personales

Solicitar confirmación sobre si la Red trata o no trata sus datos y acceder a la información que repose en bases de datos, expedientes o repositorios bajo control de la Red.

11.1.2. Actualizar y rectificar

Solicitar la corrección o actualización de datos inexactos, incompletos, desactualizados o que induzcan a error, y aportar los soportes que correspondan.

11.1.3. Solicitar supresión (eliminación) del dato

Pedir la eliminación de datos cuando: (i) no se requieran para la finalidad; (ii) se haya superado el término de conservación; (iii) el tratamiento no respete principios o normas; o (iv) se revoque la autorización y no exista deber legal/archivístico de conservación.

11.1.4. Revocar la autorización

Solicitar la revocatoria de la autorización previamente otorgada cuando sea procedente. La revocatoria no procederá cuando exista obligación legal o contractual que exija conservar el dato o cuando su conservación sea necesaria para defensa jurídica o cumplimiento de funciones públicas, debidamente justificado.

11.1.5. Ser informado sobre el uso

Solicitar información sobre el uso que la Red ha dado a sus datos personales, incluyendo finalidades, destinatarios (cuando aplique) y medidas generales de protección.

11.1.6. Presentar quejas ante la autoridad de control (SIC)

Presentar quejas por presuntas infracciones, una vez agotado el trámite interno de consultas y/o reclamos, conforme al procedimiento aquí descrito.

11.1.7. Acceso gratuito

Acceder de manera gratuita a sus datos personales al menos una vez por mes calendario y cada vez que existan cambios sustanciales de esta política, sin perjuicio de costos de reproducción o envío cuando aplique.

11.2. Procedimiento para consultas (acceso y conocimiento de datos)

11.2.1. Objeto de la consulta

La consulta es la solicitud por la cual el titular pide: (i) conocer si la Red trata datos suyos; (ii) acceder a ellos; y/o (iii) conocer el uso que se les ha dado.

11.2.2. Canales habilitados

La Red dispondrá, como mínimo, de canales institucionales para radicar consultas:

- Correo institucional o buzón funcional de protección de datos.
- Ventanilla/punto de atención presencial (si existe).
- Formulario web o sistema PQRS (si está habilitado).

11.2.3. Requisitos mínimos

La consulta debe incluir:

1. Nombre completo del solicitante.
2. Documento de identidad o mecanismo equivalente de validación.
3. Datos de contacto para respuesta.
4. Descripción clara de lo solicitado (acceso, copia, uso, fuente).
5. Si actúa un tercero: poder o acreditación de representación (representante legal, apoderado, causahabiente).

11.2.4. Verificación de identidad y legitimación (garantía de protección)

- La Red verificará la identidad del titular o la legitimación del solicitante antes de entregar información.
- En casos de alto riesgo (datos sensibles, denunciantes, testigos, NNA), se aplicarán verificaciones reforzadas y entrega minimizada a lo procedente.

11.2.5. Acceso gratuito y costos permitidos

- El acceso será gratuito al menos una vez por mes calendario y cada vez que existan cambios sustanciales de la política.
- Solo podrán cobrarse costos de reproducción o envío cuando aplique. No se cobrarán costos por búsqueda, análisis o gestión.

11.2.6. Limitaciones justificadas

Cuando la entrega integral pueda afectar derechos de terceros, reservas legales, debido proceso o seguridad de denunciantes/testigos/víctimas, la Red podrá entregar respuesta parcial (p. ej., con supresión/anonimización) y motivará la limitación.

11.3. Procedimiento para reclamos (rectificación, supresión, revocatoria e inconformidades)

11.3.1. Objeto del reclamo

El reclamo procede cuando el titular solicita rectificación, actualización, supresión, revocatoria o alega presunto incumplimiento del régimen de protección de datos.

11.3.2. Requisitos mínimos del reclamo

El reclamo debe contener:

1. Identificación del titular (nombre y documento).
2. Descripción precisa de los hechos y la solicitud (qué pide y por qué).
3. Dirección física o electrónica para notificaciones.
4. Documentos o soportes que se quieran hacer valer.
5. Acreditación de representación cuando actúe un tercero.

11.3.3. Subsanación

Si el reclamo está incompleto, se requerirá al interesado para subsanar dentro del término legal aplicable, dejando constancia. De no subsanar, se procederá conforme a las reglas internas y legales, conservando trazabilidad.

11.3.4. Plazos de respuesta

- El reclamo se atenderá en máximo quince (15) días hábiles, contados a partir del día siguiente a su recepción completa.
- Podrá prorrogarse una sola vez por ocho (8) días hábiles, con justificación informada al titular antes del vencimiento del término inicial.

11.3.5. Contenido mínimo de la respuesta

La respuesta deberá indicar:

- Decisión de fondo (procedente/improcedente/parcial).
- Acciones ejecutadas (rectificación, actualización, supresión, bloqueo, anonimización).
- Justificación jurídica y técnica cuando se niegue total o parcialmente.
- Indicación de la posibilidad de acudir a la SIC una vez agotado el trámite interno.

11.3.6. Procedencia de supresión y revocatoria (límites)

La supresión o revocatoria podrá ser improcedente cuando exista, debidamente soportado:

- Deber legal o archivístico de conservar.
- Necesidad de conservación para defensa jurídica, auditorías o control.
- Requerimiento de autoridad competente.
- Necesidad de preservar integridad de expedientes en curso.

En estos casos, la Red aplicará medidas alternativas como bloqueo, limitación de acceso, seudonimización o anonimización para divulgación, según corresponda.

11.4. Garantías reforzadas para casos sensibles, NNA y denuncias

Cuando la solicitud involucre datos sensibles, NNA o información asociada a denuncias/testigos/víctimas, la Red garantizará:

- Verificación reforzada de identidad/legitimación.
- Entrega minimizada (solo lo estrictamente procedente).
- Supresión de datos de terceros y cuasi-identificadores en copias.
- Canales seguros de respuesta y trazabilidad de entrega.
- Registro interno de accesos y actuaciones, cuando aplique.

11.5. Registro, trazabilidad y evidencia

Toda consulta o reclamo generará un registro interno con:

- Radicado, fecha, canal y responsable de trámite.
- Soportes de verificación de identidad/legitimación.
- Actuaciones realizadas y decisiones adoptadas.
- Copia de la respuesta y fecha de envío/entrega.
- Medidas aplicadas (rectificación, supresión, bloqueo, anonimización).

11.6. Quejas ante la SIC (agotamiento interno)

Una vez agotado el trámite interno de consulta y/o reclamo (o ante incumplimiento de términos), el titular podrá acudir ante la Superintendencia de Industria y Comercio (SIC) para presentar queja por presuntas infracciones al régimen de protección de datos personales, anexando el radicado y soportes del trámite interno.

12. Política de anonimización y disociación para datos sensibles (eje central)

12.1. Objeto y alcance de la anonimización/disociación

La presente política establece el estándar mínimo obligatorio para anonimizar o disociar datos personales —en especial datos sensibles, datos de NNA y datos asociados a denuncias, quejas, expedientes y evidencias— con el fin de:

- Prevenir reidentificación de titulares en productos de divulgación, transparencia o rendición de cuentas.
- Reducir riesgos de represalias, estigmatización, discriminación o revictimización.
- Garantizar circulación restringida y el principio de minimización, sin afectar indebidamente la utilidad pública de la información.

Regla clave: La seudonimización no es anonimización. Solo se considerará "anonimización" cuando el producto final no permita identificar al titular por medios razonables y se reduzca significativamente el riesgo de reidentificación.

12.2. ¿Cuándo es obligatoria la anonimización? (regla de aplicación)
La anonimización —o, como mínimo, la disociación— es obligatoria cuando la Red:
12.2.1. Publica o divulga información derivada de denuncias, quejas, PQRS o expedientes
Incluye informes, boletines, comunicados, presentaciones, piezas pedagógicas, bases de conocimiento y repositorios abiertos.
12.2.2. Realiza rendición de cuentas o reportes con ejemplos de casos
Todo caso real usado como evidencia de gestión debe presentarse anonimizando y controlando riesgo de unicidad.
12.2.3. Entrega reportes, bases o datasets a terceros sin habilitación para identificar titulares
Aplica a entregas a aliados, cooperación, academia, medios, proveedores no habilitados como encargados, u otras entidades cuando no se requiera identificación.
12.2.4. Produce contenidos audiovisuales, comunicacionales o narrativos con historias de vida o casos
Incluye foto, video, audio, pódcast, reels, entrevistas y piezas de prensa.
12.2.5. Comparte información por canales institucionales no diseñados para tratamiento sensible
Ej.: presentaciones, correos masivos, grupos, chats institucionales, cuando exista riesgo de exposición o reenvío.

12.3. Datos a anonimizar (mínimo obligatorio)
La Red deberá anonimizar, suprimir o transformar como mínimo las siguientes categorías:
12.3.1. Identificadores directos
Nombres y apellidos, número de identificación, teléfonos, direcciones, correos, firmas, huellas y biometría, fotografías de rostro, placas, licencias, códigos internos que identifiquen personas, direcciones IP, IDs de usuario, geolocalización precisa, y cualquier dato que identifique de manera inequívoca.
12.3.2. Identificadores indirectos o cuasi-identificadores
Cargo exacto, lugar de trabajo específico, barrio/vereda cuando sea identificante, entidad o dependencia específica si hace identificable, combinación de variables (edad exacta + municipio + rol), fechas puntuales, eventos singulares, rutas de movilidad, y cualquier dato que, en contexto, permita inferir identidad.
12.3.3. Datos sensibles y de especial protección
Salud (física o mental), orientación o vida sexual, biometría, convicciones, afiliaciones,

pertenencia a organizaciones, datos de víctimas/denunciantes/testigos, datos de NNA, y cualquier información cuyo uso indebido pueda generar discriminación o riesgo.

12.3.4. Metadatos y huellas digitales

Metadatos EXIF de fotos, propiedades de documentos (autor, ubicación, fecha exacta), nombres de archivos con identificación, logs exportados, enlaces con tokens o rutas internas que revelen identidad.

Regla práctica: si el documento "no tiene nombre", pero el contexto lo hace identificable, se trata como identificador indirecto.

12.4. Técnicas permitidas (selección según riesgo)

La Red aplicará técnicas según nivel de sensibilidad y riesgo de reidentificación. Se permiten, entre otras:

12.4.1. Supresión / Enmascaramiento (redacción segura)

- Tachado y eliminación real del texto (no "tapar" visualmente).
- Reemplazo por "XXX" o etiquetas ("[DENUNCIANTE]", "[TESTIGO]").
- Difuminado de rostro, señales particulares, tatuajes identificantes.
- Distorsión de voz o regrabación por narrador institucional.

12.4.2. Generalización

- Edad por rangos (18–25, 26–35), no exacta.
- Fechas por mes/trimestre o por semestre.
- Ubicación por nivel superior (localidad/departamento) cuando el municipio o barrio identifique.
- Cargo por familia ocupacional ("servidor público", "contratista", "directivo") en vez de cargo exacto.

12.4.3. Seudonimización (solo para uso interno/seguimiento)

- Códigos internos tipo "CASO-2026-001".
- Tabla de equivalencias bajo custodia separada y acceso restringido.
- Prohibido publicar tablas o claves de equivalencia.

12.4.4. Agregación

- Publicar totales, porcentajes o rangos cuando el universo sea pequeño o el contexto territorial aumente riesgo.
- Evitar desagregaciones que generen "casos únicos".

12.4.5. Perturbación / aleatorización controlada (cuando aplique)

- Ajustes leves en variables no críticas (p. ej., redondeos, rangos) para evitar unicidad, sin distorsionar el análisis.

12.4.6. Control de unicidad y criterio de k-anonimidad (regla práctica)

- No se publicarán combinaciones de variables que conviertan un caso en único en un territorio o entidad pequeña.
- Se exigirá un umbral mínimo de grupo (p. ej., "no publicar cortes con N muy bajo"), definido por el Comité de Seguridad/Privacidad.

12.5. Niveles de anonimización (estándar por sensibilidad)

Para estandarizar decisiones, se adoptan tres niveles:

12.5.1. Nivel 1 – Básico (riesgo bajo)

Supresión de identificadores directos + revisión de metadatos.

12.5.2. Nivel 2 – Reforzado (riesgo medio)
Nivel 1 + generalización de cuasi-identificadores + control de contexto territorial + revisión doble obligatoria.
12.5.3. Nivel 3 – Máximo (riesgo alto)
Nivel 2 + agregación obligatoria o narrativas sin datos de tiempo/lugar exacto + prohibición de audio/imagen identificable + prueba de reidentificación reforzada.
Aplica siempre para: NNA, víctimas, amenazas, violencia, denunciantes/testigos, salud y casos de alta notoriedad.

12.6. Procedimiento estándar de anonimización para denuncias, expedientes y evidencias
Paso 1 – Clasificación del documento/producto (12.6.1.)
- Tipo: expediente interno / informe interno / informe público / audiovisual / dataset / pieza de comunicación.
- Sensibilidad: bajo / medio / alto (alto incluye: NNA, víctimas, salud, violencia, amenazas, testigos, denunciantes, territorios pequeños).

Paso 2 – Identificación de riesgos de reidentificación (12.6.2.)
- Identificadores directos y cuasi-identificadores.
- Riesgo por contexto: notoriedad del caso, tamaño del territorio, publicaciones previas, presencia mediática.

Paso 3 – Selección de técnica y elaboración de matriz (12.6.3.)
- Matriz: campo original → técnica → campo publicado → justificación.
- Definir si se requiere seudonimización (seguimiento interno) o anonimización irreversible (publicación).

Paso 4 – Aplicación técnica segura (12.6.4.)
- Textos: edición con control de cambios, redacción segura y revisión de propiedades del documento.
- PDFs: redacción que elimine realmente el contenido (no overlays).
- Imágenes: eliminación de EXIF, difuminado de elementos identificantes.
- Audio/Video: distorsión, recorte, subtítulos sin nombres y eliminación de fondos/localizaciones identificables.

Paso 5 – Doble revisión y validación (12.6.5.)
- Revisor 1: líder del proceso misional (caso).
- Revisor 2: OPD o delegado.
- Validación: “prueba de reidentificación razonable” (¿un tercero con información pública podría inferir identidad?).

Paso 6 – Aprobación para publicación (12.6.6.)
- Para piezas públicas: aprobación de Comunicaciones + visto bueno OPD (y Comité si es nivel 3 o caso de alta notoriedad).

Paso 7 – Registro, trazabilidad y custodia (12.6.7.)
- Registrar qué se anonimizó, por qué, quién aprobó, versión publicada y fecha.
- Custodia separada de llaves de seudonimización (si existen).
- Archivo de matriz y evidencias de revisión.

12.7. Reglas especiales para piezas públicas (web/redes/informes)
12.7.1. Prohibiciones absolutas

- Prohibido publicar identidad o datos identificables de denunciantes, testigos, víctimas y NNA.
- Prohibido publicar rostros, voces, firmas, direcciones o geolocalización precisa en casos sensibles.

12.7.2. Restricciones reforzadas en casos sensibles

- Se prohíbe publicar lugares exactos, fechas exactas, dependencias específicas o detalles que permitan inferencia.
- Se privilegia agregación y generalización.

12.7.3. Casos de alta notoriedad

Cuando el caso sea ampliamente conocido o mediático:

- Se aplicará Nivel 3 – Máximo.
- Se evitarán detalles de tiempo/lugar y se usará lenguaje narrativo genérico.
- Se limitará la información a lo estrictamente necesario para fines de transparencia - educación.

12.7.4. Gestión de imagen y voz

- Si se usan historias de vida, la regla por defecto es anonimización total.
- Cualquier excepción exige autorización expresa para divulgación específica y evaluación de riesgo, sin afectar NNA ni víctimas.

12.8. Calidad, pruebas y control de reidentificación (obligatorio)

Antes de liberar un producto anonimizador:

- Verificación de eliminación de metadatos.
- Revisión de combinaciones únicas (unicidad).
- Prueba de búsqueda externa razonable (p. ej., si con municipio + cargo + fecha se identifica).
- Registro de validación y responsables.

12.9. Incumplimiento y medidas correctivas

La divulgación sin anonimización cuando sea obligatoria constituye incumplimiento grave de esta política y dará lugar a:

- Retiro inmediato del contenido,
- Activación de gestión de incidentes,
- Notificación y reporte si corresponde,
- Medidas disciplinarias/contractuales y plan de mejora.

13. Seguridad de la información y gestión de incidentes

13.1. Objetivo y regla general

La Red implementará medidas técnicas, humanas y administrativas, proporcionales al riesgo, para proteger los datos personales y evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, en concordancia con el principio de seguridad y el principio de confidencialidad del régimen colombiano de protección de datos.

13.2. Alcance

Este capítulo aplica a:

- Todas las bases de datos y repositorios físicos o digitales (denuncias, PQRS, expedientes, evidencias, audiovisual, correo institucional, nube, backups).

- Todo tratamiento realizado por integrantes de la Red, contratistas/proveedores (encargados) y terceros aliados con acceso.
- Todo el ciclo de vida del dato: recolección, almacenamiento, uso, circulación, conservación, anonimización, supresión.

13.3. Controles mínimos de seguridad (estándar base)

La Red adoptará, como mínimo, los siguientes controles:

13.3.1. Gobierno de acceso y privilegios

- Acceso por rol ("necesidad de saber"), mínimo privilegio y segregación de funciones.
- Alta/baja de usuarios con trazabilidad, especialmente al cierre de contratos o desvinculaciones.
- Autenticación reforzada cuando aplique (por ejemplo, multi-factor en repositorios críticos).

13.3.2. Protección de información y repositorios

- Cifrado o medidas equivalentes para repositorios con información sensible (denunciantes, testigos, víctimas, NNA, salud, amenazas).
- Respaldos periódicos, pruebas de restauración y controles de integridad.

13.3.3. Trazabilidad y auditoría

- Registro de accesos, exportaciones y descargas en sistemas críticos (logs).
- Monitoreo de eventos anómalos y alertas de seguridad, cuando aplique.

13.3.4. Seguridad en canales

- Prohibición de uso de cuentas personales y dispositivos no autorizados para custodia de expedientes/evidencias.
- Envío de información sensible solo por canales institucionales definidos y con controles de acceso.

13.3.5. Seguridad humana

- Compromisos de confidencialidad y formación periódica obligatoria.
- Controles para prevenir filtraciones por error humano (checklists de envío/publicación, doble revisión en contenidos con casos).

13.3.6. Gestión de proveedores (encargados)

- Cláusulas de seguridad, subencargados, incidentes, auditoría y devolución/supresión al finalizar el contrato.
- Evaluación de riesgos del proveedor según el tipo de dato tratado y criticidad del servicio.

13.4. Definición operativa de incidente de seguridad

Se entiende por incidente de seguridad cualquier evento o suceso que tenga como fin o resultado la violación de códigos de seguridad, o la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de datos personales administrados por la Red (o por sus encargados).

Ejemplos (no exhaustivos):

- Pérdida/hurto de equipos o documentos con datos personales.
- Accesos indebidos, credenciales comprometidas o filtración por correo/links.
- Publicación accidental de información sin anonimización obligatoria.
- Malware/ransomware que afecte disponibilidad o integridad.
- Entrega de datos a tercero no habilitado o por canal no autorizado.

13.5. Registro y atención de incidentes (ciclo de respuesta)

13.5.1. Deber de reporte interno inmediato

Cualquier integrante de la Red, contratista o tercero que conozca o sospeche un incidente deberá reportarlo inmediatamente al OPD (y/o al canal interno definido), sin "investigar por su cuenta" ni difundirlo por canales informales.

13.5.2. Datos mínimos del reporte interno

El reporte debe incluir, como mínimo:

1. Fecha/hora de detección y de ocurrencia estimada (si se conoce).
2. Canal/sistema afectado (PQRS, correo, repositorio, expediente físico, audiovisual, etc.).
3. Tipo de evento (pérdida, acceso no autorizado, filtración, alteración, indisponibilidad).
4. Tipo de datos comprometidos (identificadores, cuasi-identificadores, sensibles, NNA).
5. Alcance preliminar: número estimado de titulares/registros y territorios/unidades afectadas.
6. Evidencias básicas disponibles (capturas, logs, radicados, enlace, descripción del documento).
7. Medidas iniciales adoptadas (por ejemplo, desconexión, cambio de credenciales, retiro de publicación), si ya ocurrieron.

13.5.3. Gestión del incidente (fases obligatorias)

- Contención: detener la exposición (revocar accesos, retirar publicación, aislar equipo/usuario, bloquear enlaces).
- Análisis y clasificación: determinar causa probable, sistemas afectados, categorías de datos y nivel de impacto.
- Erradicación y recuperación: corregir vulnerabilidad, restaurar respaldos, revalidar accesos, asegurar integridad.
- Lecciones aprendidas: acciones correctivas/preventivas, capacitación y ajustes de control.
- Cierre formal: acta o registro de cierre con responsables y evidencias.

13.5.4. Registro de incidentes y plan de acción

La Red mantendrá un Registro de Incidentes y un Plan de Acción por incidente (correctivo y preventivo), con trazabilidad de:

- Clasificación (bajo/medio/alto), decisión de reporte externo, medidas aplicadas y fecha de cierre.
- Evidencias asociadas (logs, actas, comunicaciones, capturas, versiones retiradas/publicadas).
- Responsable del caso y aprobaciones (OPD/Comité cuando aplique).

13.6. Criterios de clasificación del impacto (para decisiones rápidas)

13.6.1. Impacto Alto (respuesta reforzada)

Se considera alto, entre otros, cuando involucra:

- Datos sensibles o NNA; denunciantes, testigos o víctimas; amenazas o violencia.
- Exposición pública (web/redes) o riesgo de represalias/revictimización.
- Compromiso de credenciales con acceso amplio o repositorios principales.

13.6.2. Impacto Medio

Acceso no autorizado controlado o limitado, con datos no sensibles, sin evidencia de exfiltración masiva, pero con riesgo de repetición.

13.6.3. Impacto Bajo

Evento aislado, contenido rápidamente, sin evidencia de acceso a datos personales o con exposición mínima y reversible.

13.7. Reporte a la Superintendencia de Industria y Comercio (SIC)

13.7.1. Plazo

El reporte de incidentes debe realizarse dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.

13.7.2. Canal de reporte (según obligación RNBD)

- Si el Responsable está obligado a reportar sus bases en el RNBD, el reporte se realiza por el RNBD.
- Si no está obligado a registrar bases en RNBD (o si se trata de un Encargado), el reporte se realiza por el módulo de "Reporte de incidentes de seguridad" dispuesto por la SIC.

13.7.3. Reserva del reporte

La información reportada sobre medidas de seguridad e incidentes no queda disponible para consulta pública en el RNBD.

13.8. Notificación a titulares (cuando exista afectación significativa)

Cuando el incidente pueda implicar un riesgo significativo para los titulares (por ejemplo, riesgo de fraude, suplantación, amenazas, discriminación, represalias, revictimización o exposición de datos sensibles/NNA), la Red notificará a los titulares afectados, en un lenguaje claro, incluyendo:

- Qué ocurrió (descripción general sin exponer más datos).
- Qué datos pudieron verse comprometidos.
- Medidas adoptadas por la Red.
- Recomendaciones prácticas de autoprotección (p. ej., cambio de contraseñas si aplica).
- Canales para ejercer derechos y obtener información.

13.9. Gobernanza y responsabilidades en incidentes

- OPD: coordina respuesta, registro, evaluación de impacto, decisiones de reporte y comunicaciones a titulares, y verifica cierre con plan de mejora.
- TI/Seguridad: contención técnica, análisis forense básico, recuperación, hardening y evidencia.
- Misional/Denuncias-PQRS: análisis de sensibilidad (denunciantes/testigos), medidas de reserva y control de divulgación.
- Comunicaciones: manejo de retiro/publicación de contenidos, mensajes externos y control de daños reputacionales bajo lineamientos del OPD.
- Comité de Seguridad/Privacidad: se activa para incidentes de impacto medio/alto, y aprueba medidas estructurales y cambios de estándar.

13.10. Evidencias mínimas de cumplimiento (auditable)

Cada incidente debe contar, como mínimo, con:

1. Registro del incidente (radicado interno).
2. Línea de tiempo de actuaciones (detección–contención–recuperación–cierre).
3. Evidencias (logs, actas, capturas, versiones retiradas).
4. Decisión de reporte a SIC (y constancia del envío si aplica).
5. Decisión de notificación a titulares (y soportes).
6. Plan de acción correctivo/preventivo y verificación de cierre.

14. Transmisión, transferencia y terceros

14.1. Regla general de control sobre terceros

La Red solo permitirá el acceso o tratamiento de datos personales por terceros cuando exista: (i) una finalidad legítima y necesaria; (ii) habilitación jurídica (autorización del titular cuando sea exigible o base legal aplicable); (iii) acuerdo/documento vinculante que delimite obligaciones; y (iv) medidas de seguridad y confidencialidad proporcionales al riesgo.

14.2. Definiciones operativas para este capítulo (distinción clave)

14.2.1. Transmisión (Responsable–Encargado)

Es la comunicación de datos a un tercero para que los trate por cuenta del Responsable, siguiendo sus instrucciones. La transmisión se soporta en un contrato de transmisión que define alcances y obligaciones.

14.2.2. Transferencia (Responsable–Responsable)

Es el envío o entrega de datos a otro Responsable (nacional o internacional) que decide sobre finalidades y medios del tratamiento. En transferencias, la Red debe verificar base jurídica, finalidades compatibles y garantías de protección.

14.2.3. Terceros

Incluye (sin limitarse a): proveedores tecnológicos, operadores de PQRS, hosting/nube, digitalizadores, custodios de archivo, productoras audiovisuales, consultores, aliados de proyectos y autoridades u otras entidades con las que se compartan datos en virtud de funciones públicas o requerimientos.

14.3. Reglas para transmisión nacional (Encargados) – contrato obligatorio

Todo tercero que actúe como Encargado del tratamiento deberá suscribir un contrato de transmisión (o cláusulas equivalentes) antes de acceder o tratar datos, de acuerdo con las exigencias reglamentarias.

14.3.1. Contenido mínimo del contrato de transmisión

El contrato deberá incluir, como mínimo:

a) Finalidades y alcance del tratamiento (qué datos, para qué, por cuánto tiempo).
b) Instrucciones documentadas del Responsable y prohibición de usos propios.
c) Medidas de seguridad (técnicas, humanas y administrativas) acordes con el nivel de riesgo.
d) Confidencialidad para el Encargado y su personal, incluso tras la terminación del vínculo.
e) Subencargados: prohibición o autorización expresa, con obligaciones equivalentes y cadena contractual.
f) Gestión de incidentes: obligación de reporte inmediato al OPD y cooperación en investigación/contención.
g) Devolución, supresión o anonimización al finalizar el servicio, salvo deber legal de conservación, con certificación.
h) Auditoría y evidencia: derecho de verificación, entrega de soportes y trazabilidad cuando aplique.
i) Ubicación del tratamiento (si hay nube o centros de datos) y reglas de acceso remoto.

j) Prohibición de transferencia a otros responsables sin autorización escrita y base jurídica válida.

14.3.2. Regla sobre información al titular en transmisiones

Cuando exista transmisión bajo contrato de Encargado en los términos reglamentarios, la operación puede no requerir consentimiento adicional del titular por ese solo hecho; en todo caso, la Red mantendrá avisos de privacidad claros y garantizará que el Encargado actúe únicamente por cuenta del Responsable.

14.4. Debida diligencia y gestión de riesgo de terceros (antes y durante)

Antes de vincular un tercero con acceso a datos personales, la Red realizará una debida diligencia proporcional al riesgo, que deberá quedar documentada:

14.4.1. Evaluación previa (mínimo)

- Tipo de datos: identificadores, sensibles, NNA, denunciantes/testigos/víctimas.
- Nivel de criticidad del servicio: acceso a repositorios principales, posibilidad de exportación masiva, acceso remoto.
- Controles del proveedor: accesos, cifrado, logs, backups, segregación, gestión de vulnerabilidades.
- Subcontratación: si existen subencargados y cómo se controlan.
- Ubicación del tratamiento y riesgos de jurisdicción si aplica (nube/soporte internacional).

14.4.2. Seguimiento y control

- Revisión periódica de cumplimiento contractual.
- Auditorías internas o verificaciones de evidencia (cuando aplique).
- Validación de eliminación/devolución al cierre del contrato.
- Control de accesos de personal entrante/saliente del proveedor.

14.5. Transferencias nacionales (a otros Responsables en Colombia)

Cuando la Red transfiera datos a otro Responsable dentro de Colombia, deberá:

a) verificar base jurídica (autorización del titular cuando sea exigible o habilitación legal);
b) asegurar finalidades compatibles y minimización;
c) documentar la transferencia (qué, a quién, para qué, bajo qué fundamento);
d) imponer salvaguardas contractuales o interinstitucionales cuando proceda (confidencialidad, seguridad, prohibición de reuso no autorizado).

14.6. Transferencias internacionales (régimen y garantías)

14.6.1. Regla de prohibición y estándar de “nivel adecuado”

La transferencia internacional de datos personales está prohibida hacia países que no proporcionen niveles adecuados de protección, salvo que concurra una excepción legal aplicable.

14.6.2. Verificación previa obligatoria

Antes de cualquier transferencia internacional, la Red deberá:

a) identificar el país de destino y evaluar si ofrece nivel adecuado conforme a estándares fijados por la autoridad;
b) verificar la base jurídica (autorización del titular cuando sea exigible) y/o la excepción legal aplicable;

c) aplicar minimización y, si el propósito no requiere identificar, preferir anonimización/disociación.

14.6.3. Garantías adecuadas para demostrar cumplimiento (cláusulas y normas corporativas)
Cuando la transferencia internacional lo requiera, la Red implementará garantías contractuales u organizacionales reconocidas como medidas apropiadas para demostrar cumplimiento, tales como:

- adopción de cláusulas contractuales y guías de implementación promovidas por autoridades y redes de protección de datos (como referencia de accountability);
- uso de Normas Corporativas Vinculantes cuando exista un grupo empresarial y el caso aplique.

La SIC ha venido desarrollando lineamientos y referencias sobre medidas y cláusulas para transferencias internacionales, lo cual la Red usará como estándar de buenas prácticas y demostración de cumplimiento.

14.6.4. Intervención de la SIC (cuando aplique)
La Red verificará si, por la naturaleza del destino, el tipo de datos o la operación concreta, se requiere actuación específica ante la autoridad (p. ej., declaraciones de conformidad, lineamientos o instrumentos aceptados), y documentará el soporte correspondiente.

14.7. Transmisión internacional (Encargados en el exterior / nube)
Cuando el Encargado esté ubicado fuera del país (o el tratamiento ocurra en infraestructura internacional), se aplicarán cumulativamente:

a) contrato de transmisión con el contenido mínimo del numeral 14.3;
b) verificación de ubicación, subencargados y cadena contractual;
c) controles reforzados de seguridad (cifrado, logs, accesos, segregación);
d) evaluación jurídica de transferencia/flujo internacional si la operación termina en un tercero que actúa como Responsable.

14.8. Reglas especiales para aliados, cooperación y academia
Cuando se compartan datos con aliados (ONG, cooperación, universidades) la regla por defecto será:

- entregar información anonimizada/disociada si el propósito no requiere identificación;
- si se requiere identificación, documentar base jurídica, firmar acuerdos de confidencialidad y seguridad, y restringir usos a finalidades pactadas;
- prohibir reidentificación, republicación y redistribución.

14.9. Publicación, medios y proveedores de comunicación
Los proveedores de comunicaciones/audiovisual que accedan a casos o historias de vida serán tratados como Encargados y deberán:

- firmar contrato de transmisión;
- cumplir la política de anonimización (numeral 12);
- asegurar que material bruto (video/audio/fotos) no se reutilice ni se conserve fuera de los plazos definidos;
- implementar controles para evitar filtraciones (accesos, almacenamiento, backups).

14.10. Registro y trazabilidad de transmisiones/transferencias
La Red mantendrá un registro interno (auditable) de:

- terceros con acceso (encargados/aliados), contratos vigentes y subencargados;
- transferencias (a qué responsable, país si aplica, finalidad, base jurídica, fecha);
- evaluaciones de riesgo realizadas y controles aplicados;
- constancias de devolución/supresión/anonimización al cierre.

15. Conservación, archivo y supresión

15.1. Regla general de conservación (limitación del almacenamiento)

La Red conservará los datos personales únicamente por el tiempo estrictamente necesario para cumplir las finalidades informadas o legalmente habilitadas, y para atender obligaciones legales, de control, auditoría, defensa jurídica y gestión documental que resulten aplicables.

En consecuencia:

- Se prohíbe la conservación indefinida "por costumbre" o por ausencia de reglas.
- La conservación deberá estar soportada en criterios objetivos: finalidad, estado del trámite, riesgos asociados y reglas de retención documental.

15.2. Criterios para definir tiempos de conservación (mínimos)

Cada veeduría, y la instancia coordinadora cuando exista repositorio unificado, definirá tiempos de conservación con base en:

15.2.1. Finalidad y necesidad operativa

- Tiempo requerido para tramitar denuncias/PQRS, realizar seguimiento y emitir productos internos o públicos (estos últimos anonimizados).

15.2.2. Obligaciones legales y de control

- Requerimientos de autoridades, organismos de control, auditorías, régimen disciplinario y demás deberes aplicables.

15.2.3. Obligaciones de archivo y gestión documental

- Aplicación de instrumentos archivísticos (Tablas de Retención Documental – TRD o equivalentes), ciclos de archivo (gestión, central, histórico) y reglas de conservación.

15.2.4. Riesgo e impacto

- Mayor plazo y controles cuando la información sea crítica para defensa jurídica o control.
- Mayor restricción y eventual anonimización/bloqueo cuando exista riesgo de represalias (denunciantes/testigos) o cuando involucre NNA o datos sensibles.

15.3. Reglas de archivo y organización documental (físico y digital)

Para garantizar integridad, trazabilidad y disponibilidad controlada, la Red aplicará:

15.3.1. Archivo físico

- Custodia en áreas definidas, con control de acceso, inventarios, préstamo documental y registro de consulta.
- Prohibición de traslado informal de expedientes sensibles fuera de los espacios autorizados.
- Manejo de evidencias con control de cadena de custodia cuando corresponda por la naturaleza del caso.

15.3.2. Archivo digital

- Repositorios institucionales autorizados (gestión documental, carpetas seguras, sistemas PQRS), evitando almacenamiento en dispositivos personales.
- Estructura de carpetas y nomenclatura que no incluya datos personales en el nombre del archivo (ej.: evitar "Denuncia_JuanPerez_Cedula.pdf").
- Control de versiones y trazabilidad (logs) en repositorios críticos.
- Gestión de metadatos (remoción de EXIF y propiedades del documento en piezas públicas).

15.3.3. Clasificación y etiquetado por nivel de sensibilidad

Los documentos se clasificarán como mínimo en: bajo/medio/alto, aplicando controles acordes (acceso, cifrado, registro de consulta, restricciones de copia/exportación).

15.4. Retención por tipo de repositorio (regla operativa)

Sin perjuicio de las TRD y normas aplicables, se adoptan reglas operativas mínimas:

15.4.1. Denuncias, PQRS y expedientes

- Conservar mientras el trámite esté abierto, más el tiempo requerido para seguimiento, control y defensa institucional, según TRD/regla interna.

15.4.2. Evidencias audiovisuales (audio/video/foto)

- Conservar por el tiempo mínimo necesario para verificación, soporte probatorio o producción interna.
- Para publicaciones, mantener solo la versión anonimizadora cuando sea posible, y restringir el material bruto.

15.4.3. Logs y trazabilidad

- Conservar por el tiempo necesario para seguridad, auditoría y análisis de incidentes, aplicando minimización y acceso restringido.

15.4.4. Copias de seguridad (backups)

- Conservar conforme a ventanas de recuperación definidas (contingencia), evitando retención excesiva.
- Asegurar que los backups estén protegidos y que existan mecanismos de supresión/expurgo cuando sea viable técnicamente.

15.5. Supresión segura (procedimientos y técnicas)

La supresión de datos personales procederá cuando se cumpla la finalidad y no exista deber legal/archivístico de conservación, o cuando sea ordenada por decisión procedente (p. ej., reclamo de titular, cuando aplique). La supresión deberá ser segura, verificable y trazable.

15.5.1. Supresión en medios digitales

- Borrado seguro: eliminación con mecanismos que impidan recuperación razonable.
- Sanitización: limpieza de soportes o sobrescritura según criticidad.
- Eliminación de metadatos: asegurar que copias, versiones y cachés no mantengan información residual.
- Expurgo en sistemas: borrar registros y copias redundantes cuando sea posible.

15.5.2. Supresión en medios físicos

- Destrucción física mediante trituración, incineración controlada o método equivalente.
- Disposición final segura, evitando reconstrucción.
- Acta o constancia de destrucción cuando corresponda por criticidad.

15.5.3. Verificación y evidencia

Toda supresión deberá dejar evidencia mínima:

- Identificación del repositorio afectado, fecha, responsable, método aplicado y alcance (qué se eliminó).
- En supresiones relevantes, constancia firmada o registro del sistema.

15.6. Bloqueo o restricción de uso (cuando no sea posible suprimir)

Cuando exista deber legal, archivístico o necesidad de defensa jurídica que impida la supresión, la Red aplicará bloqueo o restricción, consistente en:

- Mantener el dato con acceso restringido.
- Limitar su uso solo a fines de conservación obligatoria, defensa o control.

- Evitar circulación, copias o divulgación.
- Aplicar anonimización obligatoria para cualquier producto público derivado.

15.7. Supresión en repositorios unificados y con terceros

Cuando los datos estén en repositorios unificados o en manos de encargados:

- Se ejecutará la supresión conforme a contratos de transmisión (numeral 14).
- Se exigirá confirmación/certificación de supresión, devolución o anonimización.
- Se actualizarán permisos y accesos para evitar reaparición de datos por sincronización.

15.8. Gestión de solicitudes de supresión (integración con derechos del titular)

Las solicitudes de supresión se tramitarán conforme al procedimiento de reclamos (numeral 11), verificando:

- identidad/legitimación,
- procedencia y límites (deberes de conservación),
- medida aplicable (supresión, bloqueo, anonimización),
- trazabilidad y respuesta motivada.

15.9. Revisión periódica y mejora continua

La Red realizará revisiones periódicas (al menos anuales) de:

- tiempos de retención,
- consistencia entre repositorios,
- cumplimiento de supresión/bloqueo,
- y hallazgos de auditoría e incidentes,
  ajustando procedimientos y capacitación.

16. Transparencia y acceso a información pública

16.1. Propósito

La Red armonizará el derecho de acceso a la información pública con la protección de datos personales, garantizando que la transparencia se ejerza sin vulnerar derechos fundamentales como la intimidad, la seguridad, el habeas data y el debido proceso. Cuando sea necesario, la información se entregará parcialmente, aplicando anonimización/disociación o supresión de datos.

16.2. Regla general de armonización

En toda solicitud de acceso a información pública que contenga o pueda revelar datos personales, la Red aplicará esta regla:

1. Entregar la información pública que proceda.
2. Restringir o entregar parcialmente cuando la divulgación:
    - revele datos personales no necesarios para la finalidad de transparencia,
    - exponga datos sensibles o de NNA,
    - permita identificar denunciantes, testigos, víctimas o informantes,
    - afecte el debido proceso, la presunción de inocencia o investigaciones en curso,
    - genere riesgos ciertos para la seguridad o integridad de personas.

Regla operativa: si el objetivo de la solicitud puede satisfacerse sin identificar personas, se entregará en formato anonimizado o agregado.

16.3. Criterios de decisión (test de divulgación responsable)

Para decidir si se entrega total, parcial o se niega la información, la Red aplicará un análisis mínimo:

16.3.1. Necesidad y proporcionalidad

- ¿La identificación del titular es necesaria para satisfacer el interés público de la solicitud?
- ¿Puede entregarse el mismo contenido con supresión o generalización?

16.3.2. Naturaleza del dato

- Público / semiprivado / privado / sensible / NNA.
- Identificadores directos o cuasi-identificadores (ver numeral 12).

16.3.3. Riesgo de reidentificación y daño

- Contexto territorial (municipios pequeños).
- Notoriedad del caso.
- Existencia de amenazas, violencia, víctimas o testigos.
- Posible revictimización, represalias o discriminación.

16.3.4. Estado del trámite y debido proceso

- Si hay actuaciones administrativas o judiciales en curso, se evita afectar investigación, reserva y garantías procesales.

16.4. Formas de entrega (prioridad de mitigación)

Cuando la solicitud involucre datos personales, la Red priorizará las siguientes modalidades, en este orden:

16.4.1. Entrega anonimizada/disociada (preferente)

- Supresión de identificadores directos.
- Generalización de cuasi-identificadores.
- Agregación cuando el universo sea pequeño.

16.4.2. Entrega parcial (testado/redactado)

- Testado seguro en PDF y documentos (eliminación real del contenido).
- Separación de anexos con datos sensibles o de terceros.

16.4.3. Entrega agregada o estadística

- Totales, rangos, porcentajes y tendencias.
- Evitar cortes por variables que produzcan casos únicos.

16.4.4. Negación motivada

- Solo cuando la entrega, incluso parcial o anonimizada, implique un riesgo grave o una restricción legal expresa, y no sea posible mitigar.

16.5. Reglas reforzadas para denuncias y casos sensibles

En solicitudes relacionadas con denuncias, expedientes o evidencias:

- Se aplicará por defecto reserva de identidad de denunciantes, testigos y víctimas.
- No se entregará información que permita inferir identidades por combinación de datos (edad exacta + municipio + cargo + fecha).
- Se prohíbe divulgar información identificable de NNA en cualquier modalidad.
- Se privilegiará la entrega en forma agregada o con descripciones generales del caso.

16.6. Procedimiento interno para solicitudes (mínimo)

La atención de solicitudes de información pública que involucren datos personales deberá:

1. Identificar si el contenido solicitado incluye datos personales o permite inferencia.
2. Clasificar el nivel de sensibilidad (bajo/medio/alto).
3. Definir modalidad: total / parcial (testado) / anonimizada / agregada / negada motivadamente.

4. Aplicar matriz de anonimización cuando proceda (numeral 12).
5. Validación: OPD o delegado cuando sea nivel medio/alto o involucre denuncias/NNA/datos sensibles.
6. Registrar la decisión y la versión entregada.

16.7. Registro y trazabilidad

La Red mantendrá trazabilidad de:

- solicitud y radicado,
- análisis aplicado (criterios 16.3),
- decisión (entrega total/parcial/anonimizada/negada),
- versión final entregada y técnica de testado/anonimización usada,
- responsables de aprobación.

16.8. Publicación proactiva (transparencia activa) con protección de datos

En transparencia activa (web, informes, repositorios abiertos), la Red publicará información preferiblemente:

- agregada,
- anonimizada (si hay casos),
- y sin metadatos identificantes,
  evitando divulgar listados de personas o "casos únicos" que permitan inferencia.

17. Capacitación, auditoría y mejora continua

17.1. Propósito

La Red implementará un ciclo permanente de formación, verificación y mejora, orientado a asegurar el cumplimiento del régimen de protección de datos, la correcta aplicación de la anonimización/disociación, y la reducción de riesgos operativos, jurídicos y reputacionales.

17.2. Capacitación obligatoria (mínimos y periodicidad)

17.2.1. Formación anual obligatoria

La Red adoptará un plan anual de capacitación obligatoria para:

- Integrantes de la Red (funcionarios, servidores, veedores vinculados, personal de apoyo).
- Contratistas y proveedores con acceso a datos personales.
- Terceros aliados que, por su rol, traten o accedan a información personal.

17.2.2. Contenidos mínimos

El plan anual incluirá, como mínimo:

1. Principios y obligaciones del tratamiento de datos personales.
2. Derechos de los titulares y procedimientos internos (consultas/reclamos).
3. Datos sensibles y NNA: estándar reforzado, reserva y minimización.
4. Política de anonimización/disociación: técnicas, niveles y prueba de reidentificación.
5. Seguridad de la información: accesos, phishing, canales permitidos, manejo de evidencias.
6. Gestión de incidentes: detección, reporte inmediato, registro y medidas de contención.
7. Transparencia y acceso a información pública: entrega parcial y testado seguro.
8. Obligaciones contractuales con encargados y terceros.

17.2.3. Inducción y reinducción

- Inducción obligatoria al ingreso (o al inicio de contrato) antes de otorgar accesos.

- Reinducción cuando haya cambios de sistema, incidentes relevantes o actualización de política.

17.2.4. Evidencia de la capacitación

Se conservará evidencia mínima: listas de asistencia, evaluaciones, contenidos impartidos, certificaciones y fecha, asociadas al rol del participante.

17.3. Auditorías internas (periodicidad, alcance y método)

17.3.1. Auditorías semestrales

La Red realizará auditorías internas semestrales orientadas a verificar:

- Cumplimiento de la política y procedimientos.
- Atención de titulares (radicados, tiempos, respuestas).
- Contratos de transmisión y control de terceros.
- Gestión de incidentes (registro, plazos, planes de acción).
- Publicaciones y rendición de cuentas (anonimización aplicada, control de metadatos).

17.3.2. Alcance mínimo de auditoría

Al menos, se revisará:

1. Inventario de bases y flujos actualizado.
2. Control de accesos (altas/bajas, roles, trazabilidad).
3. Evidencia de autorizaciones o habilitaciones legales.
4. Matrices de anonimización y aprobaciones (nivel 2/3).
5. Cumplimiento de retención/supresión/bloqueo.
6. Proveedores: evidencia de obligaciones y reportes.

17.3.3. Metodología y productos

Cada auditoría deberá producir:

- Plan y lista de verificación (checklist).
- Hallazgos y clasificación (crítico/alto/medio/bajo).
- Recomendaciones y plan de mejora con responsables y fechas.
- Acta de cierre y verificación posterior.

17.4. Indicadores de seguimiento (KPIs mínimos)

La Red adoptará indicadores mínimos para medir desempeño, por ejemplo:

- % de personal capacitado vs. total con acceso.
- Tiempo promedio de atención de consultas y reclamos.
- Número de incidentes por tipo y tiempo de contención.
- % de publicaciones con matriz de anonimización y doble validación.
- Cumplimiento de supresión/bloqueo en muestreo semestral.
- Cumplimiento de contratos de transmisión (vigencia y evidencias).

17.5. Mejora continua y acciones correctivas/preventivas

17.5.1. Planes de mejora

Los hallazgos de auditoría, incidentes, quejas y revisiones del Comité se traducirán en planes de mejora con:

- acción definida, responsable, plazo y evidencia de cierre.

17.5.2. Gestión del cambio

Cuando se implementen nuevos sistemas, canales o repositorios, se realizará:

- evaluación de riesgos de privacidad y seguridad,
- ajustes de controles por defecto,
- actualización de formatos y avisos.

17.6. Actualización de la política

La política se actualizará cuando:

- cambie la normatividad aplicable,
- cambien los riesgos (por incidentes, amenazas, nuevos canales o alianzas),
- se integren nuevas finalidades, bases o repositorios, o
- se detecten brechas de cumplimiento.

Toda actualización deberá:

1. quedar aprobada por la instancia competente (OPD/Comité/acto interno),
2. divulgarse internamente,
3. reflejarse en avisos de privacidad y formatos, y
4. generar reinducción obligatoria cuando sea sustancial.

Citas normativas y referencias aplicables

1. Constitución Política de Colombia (1991) – Art. 15 (intimidad y habeas data), Art. 20 (libertad de informar), Art. 23 (derecho de petición). Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Constitucion/1687988.
2. Ley Estatutaria 1581 de 2012 – Régimen general de protección de datos personales (principios, derechos, responsables/encargados, datos sensibles). Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507.
3. Decreto 1377 de 2013 – Reglamenta parcialmente la Ley 1581 de 2012 (autorización, avisos de privacidad, políticas, transferencias, etc.). Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1276081.
4. Decreto Único 1074 de 2015 (Sector Comercio, Industria y Turismo) – Compila y organiza la reglamentación aplicable (incluye régimen operativo sobre protección de datos, RNBD y reglas asociadas). Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?id=30019935.
5. Decreto 886 de 2014 – Reglamenta el Registro Nacional de Bases de Datos (RNBD) (información mínima, administración, términos/condiciones). Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?id=1184150.
6. Decreto 090 de 2018 – Ajusta disposiciones sobre RNBD (universo/obligaciones y aspectos operativos). Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?id=30036646.
7. Ley 1266 de 2008 – Hábeas data (especialmente información financiera/crediticia/comercial/de servicios). Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676616.
8. Ley 2157 de 2021 – Modifica y adiciona la Ley 1266 de 2008 (fortalece el derecho al hábeas data). Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?id=30042420.
9. Ley 1098 de 2006 (Código de Infancia y Adolescencia) – Marco de protección reforzada para NNA (relevante para "interés superior" y cautelas en datos). Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1673639.
10. Ley 1878 de 2018 – Modifica artículos de la Ley 1098 de 2006 (restablecimiento de derechos y ajustes relevantes). Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/30034434.
11. Ley 1712 de 2014 – Transparencia y derecho de acceso a la información pública (armonización con reserva, intimidad y protección de datos). Consulta (SUIN-Juriscol): http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1687091.
12. Decreto 103 de 2015 – Reglamenta parcialmente la Ley 1712 de 2014 (procedimientos y deberes de publicación/entrega). Consulta (SUIN-Juriscol vía ficha): https://www.apccolombia.gov.co/normativa/decreto-no-103-de-2015 (allí contiene enlace "Ver en SUIN").
13. Ley 1755 de 2015 – Derecho fundamental de petición (trámites y términos; relevante para PQRS y solicitudes de titulares). Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/30043679.
14. Ley 594 de 2000 (Ley General de Archivos) – Gestión documental, conservación, acceso, préstamos, retención y responsabilidades de custodia. Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1663152.

15. Ley 850 de 2003 – Veedurías ciudadanas (marco de participación/control social; relevante para reglas internas de recepción y manejo de denuncias). Consulta (SUIN-Juriscol): http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1669667.
16. Ley 1757 de 2015 – Participación democrática (mecanismos, control social y fortalecimiento). Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/30019924.
17. Ley 1273 de 2009 – Delitos informáticos y protección penal de la información y los datos (riesgos, accesos indebidos, daño informático). Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699.
18. Decreto 338 de 2022 – Lineamientos de seguridad digital y gobernanza (gestión de riesgos e incidentes en entorno digital). Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?id=30043957.
19. Decreto 255 de 2022 – Normas corporativas vinculantes (BCR) y reglas asociadas a transferencias en grupos empresariales (cuando aplique). Consulta (SUIN-Juriscol): https://www.suin-juriscol.gov.co/viewDocument.asp?id=30043885.
20. Superintendencia de Industria y Comercio (SIC) – "Título V: Protección de Datos Personales" (Circular Única / instrucciones administrativas). Página oficial SIC (Sede electrónica): https://sedeelectronica.sic.gov.co/transparencia/normativa/titulo-v-0 (incluye archivo descargable).
21. SIC – Concepto/criterio oficial sobre reporte de incidentes de seguridad (incluye regla de 15 días hábiles y canal). Consulta (Sede electrónica SIC): https://sedeelectronica.sic.gov.co/publicaciones/boletin-juridico/concepto/cumplimiento-de-la-obligacion-del-reporte-de-incidentes-de-seguridad.

Referencias técnicas para anonimización

(útiles para el procedimiento, sin reemplazar la norma)

22. Archivo General de la Nación (AGN) – "Guía de Anonimización de Datos Estructurados (Conceptos generales y propuesta)" (PDF). Consulta directa: https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/Guia_de_Anonimizacion-min.pdf.
23. AGN – Nota/entrada institucional sobre la guía (contexto de publicación). Consulta: https://www.archivogeneral.gov.co/el-agn-presenta-guia-de-anonimizacion-de-datos-estructurados-conceptos-generales-y-propuesta.
24. Centro Nacional de Memoria Histórica (CNMH) – "Guía para la anonimización de datos e información no estructurada" (página institucional). Consulta: https://centrodememoriahistorica.gov.co/guia-para-la-anonimizacion-de-datos-e-informacion-no-estructurada/.
25. Archivo de los DD. HH. (plataforma CNMH/Archivo) – PDF de guía de anonimización no estructurada (cuando se requiera descarga directa/respaldos). Consulta: https://www.archivodelosddhh.gov.co/saia_release1/ws_client_oim/caja_her/documents/GuiaAnonimizacion.pdf.
26. MinTIC / datos.gov.co – Guía de Datos Abiertos en Colombia (incluye recomendaciones de publicación y cautelas de privacidad). Consulta:

https://herramientas.datos.gov.co/sites/default/files/Guia%20de%20Datos%20Abiertos%20de%20Colombia.pdf.
27. MinTIC – Guía de estándares de calidad e interoperabilidad de datos abiertos (buenas prácticas para apertura y control de calidad; útil para “publicar sin identificar”). Consulta: https://gobiernodigital.mintic.gov.co/692/articles-179118_recurso_5.pdf.