

Protocolo para la anonimización de los datos e información contenida en los archivos de inteligencia, contrainteligencia y gastos reservados - ICGR del extinto DAS.

1. OBJETIVO

Establecer los aspectos a tener en cuenta y las actividades que se deben adelantar para la anonimización de los documentos de inteligencia, contrainteligencia y gastos reservados - ICGR del extinto DAS, objeto de Intervención archivística, para el levantamiento de la reserva y desclasificación.

2. ALCANCE

El presente documento aplica para los servidores públicos de la Dirección Nacional de Inteligencia que deban realizar el proceso de anonimización de las *copias digitales de los documentos* (objetos digitales) de inteligencia, contrainteligencia y gastos reservados - ICGR del Extinto DAS, y comprende desde la recepción de estas copias digitales, provenientes del Archivo General de la Nación - AGN, pasando por la aplicación de fases de anonimización, hasta la remisión del documento digital anonimizado al AGN.

3. RESPONSABILIDADES

El/la Jefe(a) de la Oficina Jurídica es el/la responsable de velar por el cumplimiento de lo previsto para la elaboración de las versiones anonimizadas de las *copias digitales de los documentos* inteligencia, contrainteligencia y gastos reservados - ICGR del Extinto DAS, por lo cual debe coordinar lo necesario con las diferentes partes involucradas, y facilitar el proceso de recepción, trámite y entrega de los mismos.

De igual forma, de ser necesarias, debe coordinar las socializaciones o sensibilizaciones a los servidores públicos que participan de los lineamientos establecidos. Finalmente, el/la Jefe(a) de la Oficina Jurídica es quien aprueba la versión anonimizada de estas copias digitales.

De otra parte, el/la Directora(a) de Gestión Institucional, es el/la encargado(a) de suministrar los equipos (hardware y software) necesarios para elaborar las versiones anonimizadas de las *copias digitales de los documentos* de ICGR del Extinto DAS; y el/la Subdirector(a) de Asuntos

Internos y Seguridad de Activos es responsable de garantizar que en el proceso de recepción y remisión de las copias digitales objeto de anonimización no se afecte la seguridad de la información.

4. DEFINICIONES

1. **Anonimización:** La anonimización es el proceso mediante el cual se condiciona un conjunto de datos de modo que no se pueda identificar a una persona, pero pueda ser utilizada para realizar análisis técnico y científico válido sobre ese conjunto de datos (Decreto 1400 de 2025 – Desclasificación y levantamiento de la reserva de la información de inteligencia, contrainteligencia y gastos reservados del extinto DAS).
2. **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012 – Protección de Datos Personales).
3. **Información.** Se refiere a un conjunto organizado de datos contenido en cualquier documento que el extinto Departamento Administrativo de Seguridad - DAS generen, obtengan, adquieran, transformen o controlen (Ley 1712 de 2014).
4. **Información pública.** Es toda información que el extinto Departamento Administrativo de Seguridad - DAS haya generado, obtenido, adquirido, o controlado en el ejercicio de sus funciones (basado en la interpretación del literal a) del artículo 6, Ley 1712 de 2014).
5. **Información pública clasificada.** Es aquella información que estuvo en poder o custodia del extinto Departamento Administrativo de Seguridad - DAS, pero pertenece al ámbito propio, particular y sensible, privado o semiprivado de una persona natural, por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados de la intimidad, la vida, la salud o la seguridad (basado en la interpretación del literal c) del artículo 6, Ley 1712 de 2014).
6. **Intervención archivística del fondo documental del extinto DAS:** Proceso que tiene como finalidad dar una máxima publicidad a la integridad de los archivos, documentos y datos del fondo documental del extinto DAS, y consta de subprocesos archivísticos como la foliación, primeros auxilios documentales, restauración y descripción de todos los archivos, a cargo del Archivo General de la

Nación - AGN; así como, actividades de anonimización de la información contenida en ellos por parte de la Dirección Nacional de Inteligencia - DNI; para que, finalmente, el AGN genere una versión digital de consulta pública de estos archivos.

7. **Objeto digital:** Conjunto de datos binarios que permite la representación de una unidad de información (Documento Textual, Imagen digital, Video o audio digital, Base de datos, Hoja de cálculo, etc.) que tiene un identificador o nombre único y que es creado, gestionado, almacenado y reproducido mediante recursos informáticos (Acuerdo 001 2024, Anexo 1. "Definiciones". Archivo General de la Nación)
8. **Titular:** Persona natural cuyos datos personales sean objeto de tratamiento (Ley 1581 de 2012– Protección de Datos Personales).

5. CONSIDERACIONES GENERALES

De acuerdo con el artículo 11 de la Constitución Política de Colombia el derecho a la vida es inviolable; de conformidad con el artículo 15 todas las personas tienen el derecho a su intimidad personal y familiar y al uso del buen nombre; finalmente, el artículo 2 establece como deber de las autoridades del Estado proteger a todas las personas residentes en Colombia en su vida.

Lo anterior, implica que el Estado debe garantizar la protección de los derechos fundamentales a la intimidad, la vida, la salud y la seguridad de las personas en cualquier ámbito, incluso en la gestión documental y de archivo de las entidades públicas; por esta razón, los datos contenidos en documentos públicos que pongan en riesgo estos derechos deben ser protegidos antes del conocimiento al público.

Ahora, es de resaltar que, si bien esta protección Constitucional tiene una duración ilimitada, ésta reserva sólo podrá mantenerse mientras subsistan riesgos objetivos de que, al revelarla, resultara afectado de manera desproporcionada uno de los derechos que se busca proteger (Sentencia C-274 de 2013).

Por lo anterior, resulta indispensable que en cumplimiento de los parámetros Constitucionales descritos y en desarrollo del proceso de

intervención archivística del fondo documental del extinto DAS, la Dirección Nacional de Inteligencia adelante la anonimización de la información que reposa en los archivos, documentos y datos del Fondo Documental del extinto DAS en custodia del AGN.

Esta actividad de anonimización, que busca condicionar un conjunto de datos de modo que no se pueda identificar a una persona, recae sobre los datos personales de éstas, dado que con ellos se puede vincular o asociar a una o varias personas naturales determinadas o determinables.

Sobre el particular, la jurisprudencia Constitucional ha precisado que las características de los datos personales son las siguientes (Sentencia SU-139 de 2021):

- i. Se refieren a aspectos exclusivos y propios de una persona natural.
- ii. Permiten identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos.
- iii. Su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita.
- iv. Su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación.

Respecto a los datos personales, es importante indicar que guardan íntima relación con el derecho al *habeas data*, ya que, en primer lugar, es considerado una garantía del derecho a la intimidad, al proteger los datos que pertenecen a la vida privada y familiar.

Y en segundo lugar, se considera que el *habeas data* es una manifestación del libre desarrollo de la personalidad, por cuanto se fundamenta en la autodeterminación y libertad como condición indispensable para el libre desarrollo de la personalidad y en esta vía de la dignidad humana.

La anonimización como mecanismo técnico y jurídico indispensable para la salvaguarda de los derechos fundamentales de las personas.

Todo tratamiento de datos personales debe estar intrínsecamente ligado al respeto irrestricto de la dignidad humana, la intimidad y el derecho a la vida

privada. Estos principios, consagrados en instrumentos de derecho internacional como la Declaración Americana de los Derechos y Deberes del Hombre y la Convención Americana sobre Derechos Humanos, no son meras aspiraciones, sino obligaciones vinculantes que exigen la adopción de medidas efectivas para proteger a las personas de injerencias arbitrarias o abusivas en su vida personal y familiar.

En este entendido, el presente documento pretende definir un marco de actuación para los procesos de anonimización, con la obligación de proteger a los titulares de los datos y servir de garantía institucional para el derecho a la verdad.

Este proceso adquiere una dimensión de análisis jurídico especial en contextos de violaciones de derechos humanos, donde la revelación de la identidad en los documentos de inteligencia, contrainteligencia y gastos reservados - ICGR del extinto DAS puede exponer, por un lado, a las víctimas, sus familias y ciudadanos en general a graves riesgos de seguridad y/o revictimización, y, por otro lado, puede ocasionar opacidad en datos que deberían ser de público conocimiento.

Por lo tanto, analizar y comprender estos fenómenos debe partir de que la protección de la identidad es un pilar de la justicia y la reparación, y que, además, la anonimización sirve para cumplir con esta responsabilidad, ya que, es imperativo comprender los fundamentos jurídicos que rigen el tratamiento de datos personales y que dotan de legitimidad a todo el proceso.

6. CONTENIDO

6.1. Recepción de la copia digitalizada

El Archivo General de la Nación - AGN dispondrá de un espacio de almacenamiento digital, para ubicar las *copias digitales de los documentos* (objetos digitales) del archivo inteligencia, contrainteligencia y gastos reservados - ICGR del extinto DAS en su custodia, que hayan sido objeto de los procesos archivísticos de foliación, primeros auxilios documentales, restauración y descripción; dicho objeto digital se presume que es una copia digital idéntica al documento original.

Igualmente, en este espacio se entregará una copia de la descripción realizada por el AGN y se dejará la trazabilidad de la fecha y hora de la entrega del documento digital a la DNI; así como, indicar al funcionario responsable del proceso de anonimización de cada objeto digital.

6.2. Revisión y elaboración de la anonimización

El funcionario responsable de la anonimización debe verificar que los objetos digitales remitidos por el AGN puedan abrirse y se adjunte la descripción documental correspondiente; de no contar con los lineamientos establecidos, se devolverán con la observación correspondiente.

Los objetos digitales que cuente con las características completas, se le debe efectuar un registro previo a iniciar el análisis de los datos susceptibles de anonimización con el propósito de garantizar la integridad de la información, en el siguiente formato:

Formato Registro de entrega y devolución

Es de resaltar que el proceso de anonimización no debe ser concebido como un acto único, sino como una metodología compuesta por fases, que dependen una de otra, y son obligatorias.

La omisión de cualquiera de estas fases o la ejecución incompleta de cualquiera de estas etapas compromete la legalidad y la efectividad del documento anonimizado, puede dejar a los titulares de los datos en una posición de extrema vulnerabilidad. Así mismo, la inobservancia de lo descrito puede acarrear responsabilidad disciplinaria.

6.2.1. Fase de identificación del tipo de datos objeto de anonimización

La primera fase consiste en realizar un análisis de los datos contenidos en la *copia digital del documento* (objeto digital) de ICGR del extinto DAS, con el objetivo de comprender su estructura, contenido, las variables que lo componen y el contexto en el que la información fue recolectada, especialmente si se trata de información sobre víctimas de violaciones de derechos humanos.

6.2.2. Fase de identificación y clasificación de los atributos

Con base en el análisis realizado, se debe clasificar los datos objeto de anonimización de acuerdo con la tipología descrita en el **numeral 8 Tipología de Datos Objeto de Anonimización**, para clasificar cada variable (Datos de Identificación Directa, Indirecta o Sensible); esta clasificación es el diagnóstico que permite especificar qué tipo de dato dentro de estas tipologías se debe establecer como reemplazo del dato anonimizado. Ejemplo:

Fulanito Pascual = Nombre completo 1
Carrera 13 # 28-45 = Dirección de residencia 1

6.2.3. Fase de determinación y aplicación de las técnicas de anonimización.

En esta etapa se seleccionan y aplican las técnicas adecuadas para mitigar los riesgos identificados, éstas se eligen buscando un equilibrio óptimo entre la protección y la utilidad del contenido del objeto digital; de acuerdo con las siguientes técnicas:

- Técnica de supresión: ocultar por completo el dato objeto de protección.
- Técnica de generalización: reducir la precisión del dato, convirtiendo un dato exacto en un rango, porcentaje, etc.
- Técnica de perturbación: introducir modificaciones para reducir la exactitud del dato.

6.3. Evaluación del riesgo de reidentificación

Una vez aplicadas las técnicas, es obligatorio medir su efectividad, es decir, en ejercicio de una diligencia debida obligatoria para garantizar el proceso de anonimización, se debe evaluar el riesgo residual para reidentificar a los ciudadanos.

Esto exige que la Entidad considere, no solo sus propias capacidades, sino también los recursos tecnológicos y el conocimiento de terceros para realizar la reidentificación.

6.3.1. Evaluación de la utilidad de los datos

Finalmente, se debe realizar un análisis para asegurar que los datos anonimizados conservan el valor y la integridad necesarios para cumplir con su propósito; es decir que, si el proceso de anonimización vuelve inútil los demás datos del documento, se debe ajustar el equilibrio entre lo protegido y la utilidad, sin comprometer los datos personales del titular.

6.4. Remisión del documento anonimizado al AGN

Realizada la anonimización del *objeto digital* por parte del funcionario responsable de la Entidad, éste debe guardar la última versión y dejar registro de la fecha y hora de entrega y si aplica alguna observación adicional sobre el proceso de anonimización, en el siguiente formato:

Formato Registro de entrega y devolución

Acto seguido el funcionario remitirá la versión digital anonimizada al Archivo General de la Nación, para lo de su competencia.

7. Reversión del proceso de anonimización por solicitud del titular

Remitida la *copia digital del documento* (objeto digital) anonimizado al Archivo General de la Nación – AGN, para que éste lo ponga a disposición de la ciudadanía, en cumplimiento del artículo 6 del Decreto 1400 de 2025; y manifestada la voluntad del titular del dato personal anonimizado de que éste sea público, es decir, que se reverse la anonimización realizada por la Dirección Nacional de Inteligencia - DNI, el AGN debe remitir nuevamente a la DNI la versión original del objeto digital, para que se realice de nuevo el proceso de anonimización. Al realizar nuevamente este proceso la Entidad debe garantizar, por un lado, la voluntad del titular del dato, y por otro, que no se afecten derechos de terceros.

8. Tipología de Datos Objeto de Anonimización

La clasificación correcta de los datos es un paso estratégico y fundamental antes de iniciar cualquier proceso técnico de anonimización; una clasificación errónea de un dato puede llevar a un tratamiento técnico insuficiente, resultando en un documento que, aunque aparente ser anónimo, permite la reidentificación.

Esto no solo constituye una vulneración de la normativa de protección de datos, sino que puede implicar una revictimización de los titulares, exponiéndolos a riesgos de discriminación o persecución; así como, posibles afectaciones a la vida e integridad personal de los involucrados.

8.1. Datos de Identificación Directa

Estos son los atributos que, por sí solos, permiten la identificación inequívoca de una persona, su tratamiento requiere el máximo nivel de protección, y generalmente son los primeros datos en ser suprimidos o transformados en un proceso de anonimización. Ejemplos:

- Nombre completo
- Número de cédula de ciudadanía o documento de identidad
- Número de Identificación Tributaria (NIT)
- Dirección de residencia
- Número de Tarjeta Profesional

8.2. Datos de Identificación Indirecta

Estos datos, aunque no identifican a una persona de forma aislada, pueden llevar a su reidentificación cuando se cruzan entre sí o con otras fuentes de información disponibles, el riesgo que representan es a menudo subestimado, pero su correcta gestión es clave para una anonimización efectiva. Ejemplo:

- En un municipio determinado, la combinación de variables como el nivel de escolaridad, la ocupación laboral y el ingreso promedio mensual puede delinear un perfil tan específico que permita identificar a un ciudadano concreto en esa comunidad.

8.3. Datos Sensibles

Esta categoría comprende la información más íntima de una persona, cuyo uso indebido puede generar discriminación y vulnerar su dignidad, esta categoría es de máxima relevancia en el tratamiento de archivos, donde datos como la pertenencia a organizaciones de derechos humanos no son meramente informativos, sino que constituyen parte del análisis de base para una posible recolección ilegal de información. Ejemplos:

- Origen racial o étnico
- Orientación política
- Convicciones religiosas o filosóficas
- Pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición
- Datos relativos a la salud
- Datos sobre la vida sexual
- Datos biométricos

9. Aprobación de los documentos anonimizados

El funcionario responsable de la elaboración de la *copia digital del documento* (objeto digital) anonimizado, debe remitir el formato de registro del proceso a el/la Jefe de la Oficina jurídica para la correspondiente revisión y aprobación de dichas anonimizaciones.

Esta aprobación se realiza en el formato:

Formato de aprobación

10. Documentos de referencia

1. Consejo Internacional de Archivos. (2008). *Políticas archivísticas para la defensa de los derechos humanos sobre gestión de los archivos de los servicios de seguridad del Estado de los desaparecidos regímenes represivos*. Fundación 10 de Marzo.
2. Grupo de Trabajo de Protección de Datos del Artículo 29. (2014, 10 de abril). *Dictamen 05/2014 sobre técnicas de anonimización*. Comisión Europea. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf
3. Organización de los Estados Americanos. (2021). *Principios actualizados sobre la privacidad y la protección de datos personales*. https://www.oas.org/es/sla/ddi/docs/CJI-doc_638-21_rev1.pdf
4. Naciones Unidas. (2024, 13 de marzo). *Política de protección y privacidad de los datos de la Secretaría de las Naciones Unidas*

- (Boletín del Secretario General ST/SGB/2024/3).
<https://docs.un.org/es/st/SGB/2024/3>
5. Unidad para la Atención e Reparación Integral a las Víctimas. (2025). *Lineamiento de anonimización de datos* (Código: 140.06.16-13, Versión 01). <https://www.unidadvictimas.gov.co/wp-content/uploads/2025/09/Lineamiento-de-Anonimizacion-de-Datos-V1.pdf>
 6. Agencia Española de Protección de Datos. (2016). *Orientaciones y garantías en los procesos de anonimización de datos personales*. <https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf>
 7. Departamento Administrativo Nacional de Estadística. (2023). *Guía de anonimización de datos estructurados* (Versión 01). <https://www.dane.gov.co/files/acerca-del-dane/gestion-etica-de-datos/Guia-de-Anonimizacion-de-Datos-Estructurados.pdf>
 8. Agencia Española de Protección de Datos y Personal Data Protection Commission de Singapur. (2018). *Guía básica de anonimización*. <https://www.aepd.es/sites/default/files/2019-09/guia-basica-anonimizacion.pdf>
 9. Centro Nacional de Memoria Histórica. (2020). *Guías para la anonimización de datos e información no estructurada*. Editorial CNMH. <https://centrodememoriahistorica.gov.co/guias-para-la-anonimizacion-de-datos-e-informacion-no-estructurada/>
 10. Instituto Colombiano de Bienestar Familiar. (2021). *Guía metodológica para la anonimización de registros* (G3.MPA1.P4.P2.G2, Versión 01). <https://www.icbf.gov.co/guia-metodologica-para-la-anonimizacion-de-registros>
 11. Agencia para la Educación Superior, la Ciencia y la Tecnología. (2024). *Guía para la anonimización de datos estructurados*. <https://agenciaatenea.gov.co/transparencia/gestion-de-datos/guia-anonimizacion>
 12. Agencia Española de Protección de Datos. (2021). *10 malentendidos relacionados con la anonimización*. <https://www.aepd.es/sites/default/files/2021-04/10-malentendidos-anonimizacion.pdf>