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 digitalizadas de los documentos físicos originales* (objetos digitales) de inteligencia, contrainteligencia y gastos reservados – ICGR del Extinto DAS, y comprende desde la recepción de estas copias *digitalizadas*, 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 digitalizadas de los documentos originales de* 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 digitalizadas*.

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 digitalizadas 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 digitalizadas 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, descripción y digitalización 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).
9. **Riesgo residual de reidentificación:** Es la probabilidad de que una persona determinada o determinable pueda ser individualizada, identificada o vinculada nuevamente a sus datos originales, después de haber aplicado el proceso de anonimización.
10. **Utilidad Documental:** Es el grado de valor, validez analítica y funcionalidad

que conserva un documento para cumplir con la finalidad pública, estadística, de transparencia o de investigación que motivó su tratamiento, tras haber sido sometido a un proceso de anonimización.

5. CONSIDERACIONES GENERALES

La anonimización y el derecho a la verdad, justicia, reparación, garantías de no repetición y la memoria histórica

La aplicación del presente Protocolo se regirá por un enfoque de derechos humanos, justicia transicional y centralidad de las víctimas. En consecuencia, las decisiones de anonimización no podrán afectar el derecho a la verdad, la memoria histórica, la investigación judicial, la reparación integral de las víctimas ni las garantías de no repetición. Toda decisión de anonimización deberá justificarse explícitamente a la luz de estos principios, y en caso de tensión entre la protección de datos personales y el derecho a la verdad, se aplicará el criterio de proporcionalidad previsto en el numeral 6.2.4 del presente Protocolo.

La protección de datos personales como garantía de otros derechos

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, esta 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.

Criterios Diferenciales entre Víctimas y Agentes Estatales para el proceso de Anonimización

Respecto de víctimas reconocidas de actividades ilegales del extinto DAS

En cuanto a víctimas, el proceso de anonimización debe aplicarse como regla general para su protección, anonimizando por defecto los datos de identificación directa, indirecta o sensible; así mismo, en la etapa de control de calidad de los documentos anonimizados se debe realizar una evaluación reforzada sobre los riesgos de reidentificación.

Es de anotar que, la víctima conserva la decisión sobre la publicación de su identidad, en este entendido, puede solicitar expresamente que su nombre aparezca cuando así lo considere funcional a su derecho a la verdad, o puede solicitar la supresión de sus datos en ejercicio del derecho a la autodeterminación informativa.

Respecto de servidores públicos y funcionarios del DAS

Cuando la conducta del servidor público o funcionario del extinto DAS fue o es relevante para el debate público y constituyó una violación de derechos humanos, una práctica institucional ilícita o un hecho judicialmente relevante, podría no operar la anonimización automática.

Sin embargo, cuando la DNI desconozca el nivel de responsabilidad de un servidor público o funcionario del extinto DAS, o cuando este no conste en sentencias judiciales, fallos disciplinarios u otra documentación oficial competente, a la Entidad no le corresponde realizar valoraciones investigativas ni juicios de responsabilidad que exceden su competencia técnica.

Ahora bien, para que la DNI tenga conocimiento sobre dicha responsabilidad, debe existir de manera previa al inicio del proceso de anonimización de cada objeto digital, información verificable que den cuenta de esto (listados de servidores públicos o funcionarios del DAS, sentencias penales, fallos disciplinarios, constancias de la Corte IDH).

Para ello, las instancias estatales competentes de acompañamiento y supervisión al cumplimiento del Decreto 1400 de 2025 deben construir y mantener actualizado un

listado que contenga esta información y compartirlo con la DNI para su correspondiente aplicación.

Aunado a lo anterior y con relación a la responsabilidad de servidores públicos o funcionarios del extinto DAS en actividades ilegales, existen tres niveles a saber:

Nivel 1 - Nivel decisional: corresponde a directores, subdirectores, jefes de grupo, oficiales de enlace con autoridad de firma, quienes aprobaron u ordenaron operaciones. En actividades, misiones u operaciones del extinto DAS calificadas como ilícitas por sentencia judicial, fallo disciplinario o documentación oficial competente, es necesario que la identidad de quienes ejercían estos cargos no sea anonimizada, dado que la posición jerárquica implica conocimiento presumible.

Nivel 2 - Nivel ejecutor con responsabilidad verificada: corresponde a analistas, oficiales de caso, detectives, agentes de campo, técnicos en interceptación, analistas financieros que hayan sido penalmente condenados, disciplinariamente sancionados, o identificados por autoridad judicial como ejecutores dolosos, por actuaciones en el ejercicio de sus funciones en el extinto DAS; frente a ellos, es necesario que su identidad no sea anonimizada.

Nivel 3 - Nivel ejecutor sin responsabilidad verificada: corresponde a la persona que ejecutó actividades sin constancia de conocimiento de la ilegalidad ni proceso en su contra; frente a estas personas es necesario que su identidad sea anonimizada, sin embargo, posteriormente puede reversase el proceso de anonimización si surge proceso judicial o disciplinario que denote la responsabilidad.

Clasificación por defecto en Nivel 3 con reclasificación posterior: dada la magnitud del fondo documental del extinto DAS, así como, para evitar la sobreexposición de servidores públicos o funcionarios sin responsabilidad determinada, y para que la DNI no asuma funciones de calificación que son propias de las autoridades judiciales y disciplinarias; en el proceso de anonimización de que trata el presente protocolo se debe asumir por defecto la protección (anonimización en Nivel 3), sin intentar inferir o presumir responsabilidades frente a cualquier servidor público o funcionario del extinto DAS, con reclasificación a Niveles 1 o 2 cuando la DNI reciba por parte de la instancia competente la información que corresponda.

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 digitalizadas de los documentos originales* (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, referenciar 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 (Matriz técnica, descriptiva y Hash), 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:

Anonimización - Control de Recepción y Entrega

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 procesada, los anteriores criterios deben ser analizados de forma implícita, así:

a) La estructura del documento. Se debe determinar si los documentos son estructurados (bases de datos, archivos Excel, etc.), semiestructurados (formularios, plantillas, modelos, etc.) o no estructurados (documentos escritos en texto libre). Sin embargo, se resalta que el proceso de anonimización regulado en este protocolo es realizado sobre copias

digitalizadas de los documentos físicos originales.

b) El contenido del documento. Se debe analizar la información escrita en el documento para clasificarlo de acuerdo con su naturaleza (información pública, clasificada o reservada de acuerdo con la normatividad vigente).

   En este entendido, si el contenido del documento es información de acceso público (revistas, periódicos, etc.), el proceso de anonimización no debe realizarse; si la información es clasificada o reservada deben analizase los datos que permitan la identificación de terceros y pongan en riesgo bienes jurídicos como la vida, seguridad personal, la intimidad y el buen nombre de estos.

c) Las variables que componen el documento. Este criterio sirve para reconocer riesgos de reidentificación, a través de variables que de forma aislada no identifican a una persona, pero combinadas sí. Por ello, se debe realizar un tratamiento diferencial con este tipo de variables, ya que estos equivalen a datos de identificación directo cuando se refieren, por ejemplo, a roles comunitarios (Gobernador del Cabildo, Líder ambiental), comunidades pequeñas o zonas de conflicto delimitadas (veredas, corregimientos, barrios específicos).

d) El contexto en el que la información fue procesada en el documento. Se debe analizar si la información contenida en el documento fue suministrada, por ejemplo, por una fuente humana o una persona reinsertada de un grupo al margen de la ley bajo estrictas promesas de reserva; o por un proceso de infiltración, que evidencie a la persona que poseía dicha información.

Los anteriores criterios deber tener un énfasis especial si se trata de información sobre víctimas de violaciones de derechos humanos, con el fin de que no se configure una revictimización por el documento anonimizado y, al tiempo, se garantice el derecho a la verdad; por ello se debe observar lo siguiente:

- En documentos no estructurados, la estructura gramatical y lógica y la secuencia cronológica no deben alterarse con la anonimización, dado que esto puede descontextualizar el documento, afectando el derecho a la verdad.
- La información o datos que relaten el daño específico sufrido por una persona víctima (violencia sexual, tortura, etc.) deben protegerse, cuando el dato se logre vincular de manera directa o indirecta con dicha persona.
- La información o datos que describan circunstancias íntimas que no aporten valor al documento deben ser suprimidos para proteger la dignidad de la víctima.
- La información o datos que den cuenta de los hechos, las estructuras jerárquicas y las conductas por fuera del marco legal deben permanecer legibles y claras en el contenido final del documento anonimizado.
- El documento anonimizado debe servir para hacer pedagogía, memoria

histórica y rendición de cuentas; es decir, el funcionario debe equilibrar la cantidad de información de contexto que se puede dejar (nombres de bloques armados, periodos presidenciales) para alimentar la verdad sin vulnerar la esfera íntima de las personas.

6.2.2. Fase de identificación y clasificación de los datos anonimizados

Con base en el análisis realizado, se deben clasificar los datos objeto de anonimización de acuerdo con la tipología descrita en el **numeral 8 Tipología de Datos Objeto de Anonimización**, para identificar cada variable (Datos de Identificación Directa, Indirecta o Sensible); esta clasificación es el diagnóstico que permite al funcionario de la Oficina Jurídica especificar qué tipo de dato dentro de estas tipologías se debe establecer como reemplazo del dato anonimizado, sustituyéndolo en su lugar por etiquetas que se sobreponen en el texto anonimizado.

6.2.3. Fase de aplicación de la técnica de anonimización (supresión).

En esta etapa se selecciona y aplica la técnica de anonimización denominada supresión, con ella se busca ocultar por completo el dato objeto de protección para mitigar los riesgos identificados, esta técnica se elige dado que los objetos digitales que el AGN remite para el proceso de anonimización contienen datos e información no estructurada, y al ser éstas copias digitalizadas de los documentos originales que reposan en el archivo ICGR del extinto DAS, las otras técnicas de anonimización que pueden aplicarse a datos e información no estructurada, no brindan el equilibrio óptimo entre la protección y la utilidad del contenido del objeto digital.

Ahora bien, es importante aclarar que la técnica de *supresión* que se reglamenta en el presente protocolo es una *combinación*[1] de las técnicas de *codificación*[2], ya que, el dato anonimizado se sustituye por etiquetas preestablecidas; y la técnica de *seudonimización*[3], puesto que internamente se conserva una tabla de correspondencia para hacer la reclasificación de los datos de agentes estatales cuando a estos se les determine el grado de responsabilidad y se informe a la DNI, o se deba reversar la anonimización por solicitud del titular de los datos.

A continuación, se muestra una imagen representativa de un documento con la aplicación de la técnica de supresión:

[1] Borrador de los LINEAMIENTOS PARA LA ANONIMIZACIÓN DE INFORMACIÓN NO ESTRUCTURADA EN DOCUMENTOS DE ARCHIVO, Archivo General de la Nación "Jorge Palacios Preciado". **Numeral 9.9 Combinación de técnicas y criterios de selección.**
[2] Borrador de los LINEAMIENTOS PARA LA ANONIMIZACIÓN DE INFORMACIÓN NO ESTRUCTURADA EN DOCUMENTOS DE ARCHIVO, Archivo General de la Nación "Jorge Palacios Preciado". **Numeral 9.2 Sustitución por etiquetas, codificación y tokenización semántica**.
[3] Borrador de los LINEAMIENTOS PARA LA ANONIMIZACIÓN DE INFORMACIÓN NO ESTRUCTURADA EN DOCUMENTOS DE ARCHIVO, Archivo General de la Nación "Jorge Palacios Preciado". **Numeral 9.2.1 Seudonimización controlada.**

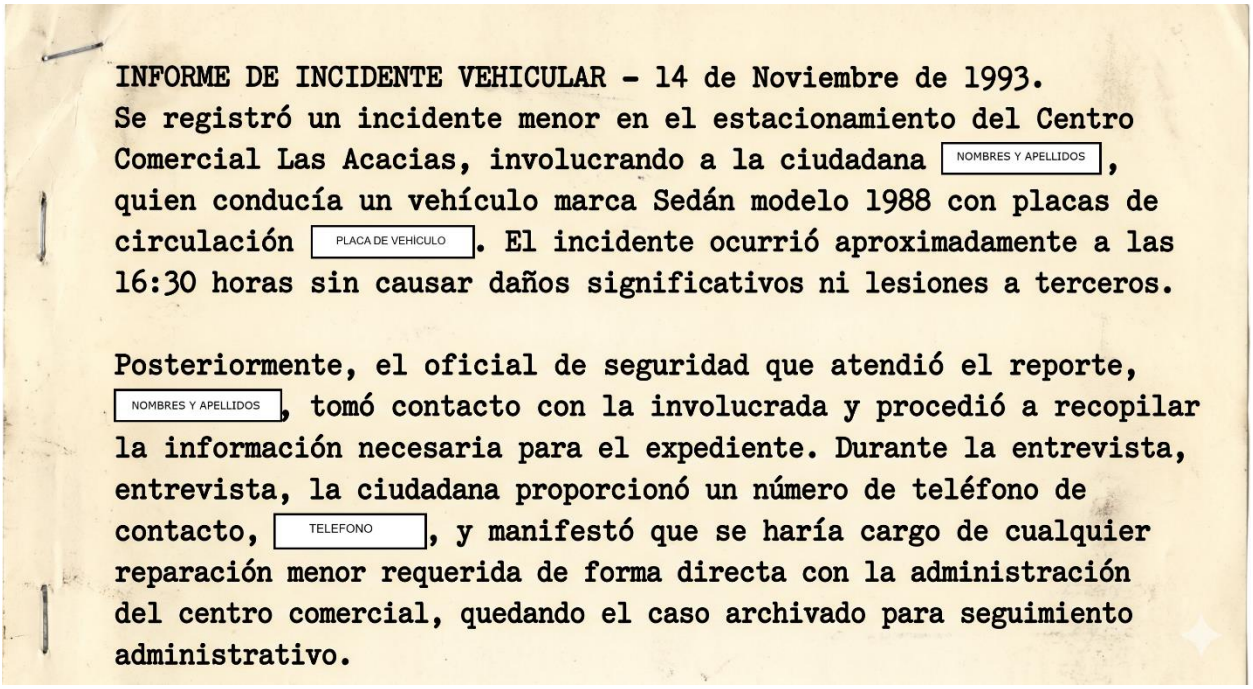

Imagen ejemplo donde se muestra el resultado de un documento anonimizado en el cual se protegen los nombres y apellidos de dos (2) personas, las placas de un (1) vehículo y un (1) número de teléfono

6.2.4. Test de proporcionalidad y necesidad.

En la matriz de *Anonimización - Control de Recepción y Entrega* que diligencian los funcionarios de la DNI al realizar este proceso, se debe establecer (i) la tipología del dato anonimizado (datos de identificación directa, indirecta o sensible), (ii) el dato específico a anonimizar y su relación con el titular; y finalmente, (iii) se justifica por qué se debe proteger este dato en el contexto del documento. La selección de estos tres datos sirve de sustento para realizar el test de proporcionalidad, puesto que de manera específica el funcionario debe argumentar su decisión, con base en el dato anonimizado, la relación de este dato en el contexto del documento, y como esto puede generar un riesgo para el titular.

6.3. Control de calidad

Las actividades de control de calidad dentro del proceso de anonimización corresponden a la *Evaluación del riesgo de reidentificación* y a la *Evaluación de la utilidad de los datos*, en esta etapa se analiza el riesgo de reidentificación y la utilidad

documental de los objetos digitales a fin de equilibrar protección de los datos con el acceso a la información.

Este control de calidad lo ejerce un funcionario diferente al que realizo la anonimización en primera medida, y este funcionario puede solicitar los ajustes necesarios para que no se materialice una sobreanonimización o en su defecto se protejan datos que se dejaron de anonimizar.

6.3.1. Evaluación del riesgo de reidentificación

Una vez aplicada la técnica de supresión, 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; por ello, un funcionario diferente al designado para realizar la anonimización debe analizar el documento nuevamente, para verificar que ningún dato de identificación directa, indirecta o sensible haya sido omitido en el proceso.

El funcionario designado para la evaluación del riesgo de reidentificación debe analizar todas las carpetas contenidas en una unidad de conservación documental (caja), con el propósito que tenga el mayor contexto sobre los datos objeto de anonimización.

Para realizar el presente análisis se establecen los siguientes criterios cualitativos de evaluación del riesgo, para que el servidor público designado para realizar el control de calidad, verifique:

a) Que la información remanente en el texto no permita separar o "aislar" a una persona del resto de la población, convirtiéndolo en un sujeto único dentro del relato (Imposibilidad de Singularización).

b) Que los datos de identificación indirectos (como fechas, lugares, cargos, iniciales) hayan sido anonimizados de tal forma que no permitan conectar un documento con otras bases de datos públicas o portales web (Imposibilidad de Vinculación).

c) Que no se puedan deducir las identidades a partir del contexto o la narrativa interna del documento (Imposibilidad de Inferencia).

Aclaración sobre el nivel de riesgo de reidentificación para el proceso de anonimización adelantado en cumplimiento del Decreto 1400 de 2025: la DNI reconoce los siguientes aspectos sobre los riesgos de reidentificación de los datos e información contenida en los archivos del fondo documental del extinto DAS:

- Los documentos contenidos en los archivos del extinto DAS objeto de anonimización han sido consultados por autoridades judiciales, disciplinarias, fiscales o entidades del Sistema Integral de Verdad, Justicia, Reparación y No Repetición, e incorporados en sus procesos archivísticos; por lo menos desde julio de 2014 con la expedición del Decreto 1303 de 2014.

- De conformidad con los numerales 4.3 y 4.4 del artículo 4º del Decreto 1400 de 2025, el proceso de anonimización a cargo de la DNI se aplica sobre las versiones digitalizadas de los archivos, documentos y datos del Fondo Documental del extinto DAS, es decir, que estos se mantienen originales y sin alterar, en aras de su integridad y protección.

- En cumplimiento del artículo 6º del Decreto 1400 de 2025 los archivos, documentos y datos del Fondo Documental del Extinto DAS se pondrán a disposición de la ciudadanía en versión digital de consulta pública, una vez se haya surtido la intervención archivística de dicho fondo documental.

- Finalmente, el artículo 7º del Decreto 1400 de 2025 establece que los archivos, documentos y datos del Fondo Documental del Extinto DAS, por su carácter de documentos históricos y Patrimonio Documental de la Nación, estarán bajo la administración, custodia y protección del AGN; y es a dicha Entidad a quien corresponde garantizar la inalterabilidad de la información contenida en los documentos originales que conforman el Fondo Documental del Extinto DAS.

6.3.2. Evaluación de la utilidad de los datos

En esta etapa del proceso de calidad, 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.

La utilidad de los datos contenida en un documento busca la preservación de la estructura esencial de la información (relaciones, tendencias, coherencia gramatical y jurídica); el proceso óptimo de anonimización busca maximizar la protección de la privacidad minimizando la pérdida de esta utilidad, garantizando que el documento final siga siendo apto para el análisis, sin desnaturalizar su contenido sustancial.

Finalmente, se debe tener en cuenta que el propósito de la intervención archivística es poner a disposición de la ciudadanía la versión digital de consulta pública de los archivos de ICGR del extinto DAS, una vez se haya surtido el procedimiento descrito, es decir los procesos archivísticos y los de anonimización (Articulo 6, Decreto 1400 de 2025); dirigido por un enfoque de derechos humanos, justicia transicional y centralidad de las víctimas.

6.4. Remisión del documento anonimizado al AGN

Realizada la anonimización del *objeto digital* por parte del funcionario responsable de la DNI, 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 y de control de calidad, en el siguiente formato:

Anonimización - Control de Recepción y Entrega

Acto seguido el funcionario remitirá la versión digital anonimizada al Archivo General de la Nación para lo de su competencia, estableciendo el código Hash SHA 256 de cada objeto digital.

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.

Es de anotar que el procedimiento de reversión de la anonimización, es exclusivamente por solicitud del titular del dato, ya que, es quien tiene la facultad de hacer efectivo su derecho, en este sentido, la DNI únicamente puede materializar la solicitud de proteger o desproteger si existe previa solicitud y sobre los archivos que tenga en proceso de anonimización; si las copias de los archivos digitales todavía no han sido remitidos por el AGN a la DNI (por la gradualidad del proceso) o si estos han sido devueltos al AGN (una vez realizada la anonimización), dicha solicitud debe ser trasladada por competencia al Archivo General para su gestión pertinente.

Los ciudadanos interesados en ejercer esta facultad pueden realizar a través de los mecanismos de contacto establecidos por la Entidad, contactenos@dni.gov.co.

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.

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.

A continuación, se enlistan tipos de datos personales directos e indirectos objeto del proceso de anonimización; no obstante, es importante advertir que la siguiente tipología no debe interpretarse de manera literal ni restrictiva, sino meramente enunciativa. Algunos datos personales son dinámicos en cuanto a su clasificación, dependiendo del contexto, la finalidad del tratamiento y la combinación con otros datos, un dato que en principio es público puede adquirir el carácter de semiprivado, privado o incluso sensible.

1. ACTIVIDAD COMERCIAL
2. ACTIVIDAD ECONÓMICA
3. ACTIVIDAD PROFESIONAL
4. AFILIACIÓN EPS
5. ANTECEDENTES DISCIPLINARIOS
6. ANTECEDENTES JUDICIALES
7. CORREO ELECTRÓNICO
8. DATOS BIOMÉTRICOS
9. DATOS DE SALUD
10. DATOS FINANCIEROS
11. DATOS SENSIBLES
12. DATOS SOCIOECONOMICOS
13. DESCRIPCION MORFOLOGICA
14. DIRECCION
15. EDAD
16. ESTADO CIVIL
17. FECHA Y LUGAR DE EXPEDICIÓN
18. FIRMA
19. HISTORIA LABORAL
20. HISTORIAL ACADÉMICO

21. IDENTIFICACIÓN INDIRECTA
22. IDENTIFICACIÓN TRIBUTARIA
23. INFORMACIÓN TRIBUTARIA
24. LUGAR Y FECHA DE NACIMIENTO
25. NACIONALIDAD
26. NOMBRES Y APELLIDOS
27. NÚMERO DE IDENTIFICACIÓN
28. PLACA DE VEHÍCULO
29. ROSTRO
30. SEXO
31. SISTEMAS DE INFORMACIÓN
32. TARJETA PROFESIONAL
33. TELÉFONO

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

En esta categoría especial de protección, se incluye igualmente los **datos relativos a los niños, niñas y adolescentes**, ya que estos requieren protección total e irrestricta, independientemente del contexto en que aparezcan en el documento. Los datos de los niños, niñas y adolescentes también contienen los datos de sus representantes legales, defensores y agentes oficiosos cuando su identificación permita inferir la identidad del menor.

9. Matriz de anonimización

Todo proceso de anonimización tendrá trazabilidad completa, a través de la matriz de anonimización, en ella se describirán los siguientes datos:

Categoría	Nombre de la Columna	Descripción / Propósito
Identificación	ID de Registro	Código único DNI para cada proceso, ej. ANDAS-2026-001-(iniciales de los nombre y apellidos del funcionario)
	Nombre del Archivo Original	Nombre tal cual se recibe el documento.
	Formato de Entrada	PDF, Imagen (OCR), Word, etc.
Recepción	Fecha y Hora de Recepción	Momento exacto en que ingresa al flujo de anonimización.
	Fuente / Remisor	Entidad, dependencia o persona que remite el archivo.
	Nivel de Calificación	Calificación (Público, clasificado, reservado).
	Hash del Archivo (SHA-256)	Código único para garantizar la integridad del archivo recibido.
Proceso Técnico	Responsable de Ejecución	Funcionario que realiza la anonimización.
	Técnica Aplicada	(P. ej. Supresión, codificación, Seudonimización).
	Software/Herramienta	Versión del script o herramienta utilizada (ej. Python v1.2).
	Tipología de Datos Objeto de Anonimización	Datos de identificacion directa, indirecta o sensible.
	Dato Anonimizado	Dato protegido del objeto digital
	Justificación de la anonimización	Razones que justifiquen la anonimización
	Número de la imagen dentro del objeto digital	Número de la página dentro del archivo (incluyendo reverso y anverso)
	Consecutivo del dato anonimizado	Consecutivo del dato anonimizado dentro de cada página del objeto digital
Control de Calidad	Fecha de Finalización	Cuando se terminó de procesar.

Dirección: Carrera 16 A # 30 17
Casa Teusaquillo
Bogotá D.C. – Colombia
Código Postal: 110311
PBX: (+57) 601 432 0000
Línea Gratuita Nacional: 01 8000 411300
www.dni.gov.co

	Verificación de Reidentificación	Resultado del test de riesgo de re-identificación (Aprobado/Fallido).
	Nombre del Archivo Final	Nombre del archivo ya anonimizado.
Entrega	Fecha de Devolución	Cuando se entrega el archivo final al AGN.
	Ruta de Entrega al AGN	Carpeta segura destinada por el AGN
	Hash del Archivo (SHA-256)	Código único para garantizar la integridad del archivo devuelto.
Observaciones del responsable	Observaciones	Notas sobre dificultades técnicas, claridades o excepciones.
Observaciones de calidad	Observaciones	Notas sobre dificultades técnicas, claridades o excepciones.

10. 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:

Anonimización - Control de Recepción y Entrega

11. Documentos de referencia

1. Presidencia de la República de Colombia. (2025, 22 de diciembre). *Decreto 1400 de 2025, por el cual se desclasifica y levanta la reserva de los archivos de inteligencia, contrainteligencia y gastos reservados del extinto Departamento Administrativo de Seguridad (DAS)*. Diario Oficial No. 53.345. https://www.suin-juriscol.gov.co/viewDocument.asp?id=30056012
2. 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.
3. 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
4. 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

5. 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
6. 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
7. 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
8. 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
9. 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
10. 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/
11. 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
12. 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
13. 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
14. Corte Interamericana de Derechos Humanos. (2023). *Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" (CAJAR) Vs.*

Colombia. Excepciones Preliminares, Fondo, Reparaciones y Costas. Serie C No. 515. https://www.corteidh.or.cr/docs/casos/articulos/seriec_515_esp.pdf

Dirección: Carrera 16 A # 30 17
Casa Teusaquillo
Bogotá D.C. – Colombia
Código Postal: 110311
PBX: (+57) 601 432 0000
Línea Gratuita Nacional: 01 8000 411300
www.dni.gov.co