



**Unidad para
las Víctimas**



Lineamiento de Anonimización de datos

Seguridad de la Información

2025

Oficina de Tecnologías de la Información

 Unidad para las Víctimas	LINEAMIENTO DE ANONIMIZACIÓN DE DATOS	Código: 140,06,16-13
	GESTION DE LA INFORMACION	Versión: 01
	PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACION	Fecha: 28/08/2025 Página 2 de 7

1. INTRODUCCIÓN

En el marco de la Política Nacional de Explotación de Datos CONPES 3920 de 2018 (Consejo Nacional de Política Económica y Social - CONPES, 2018) y la Política de Transformación Digital e Inteligencia Artificial CONPES 3975 de 2019, se reconoce el potencial que tienen los datos como activo para la generación de valor social y económico. Por tal motivo, uno de sus objetivos para la Unidad para las Víctimas, es masificar la disponibilidad de los datos públicos digitales accesibles, usables y de calidad. En ese sentido, se identifica la necesidad de fortalecer la apertura de datos para su reutilización, salvaguardando los principios reconocidos por la legislación en materia de transparencia y protección de datos personales.

De acuerdo con la ley de protección de datos 1581 de 2012 se establecen los principios, finalidades y tratamiento para la protección de datos personales. La finalidad de la anonimización de los datos es, evitar la identificación de las personas y reducir su probabilidad de Re-identificación sin afectar la veracidad de los resultados y la utilidad de los datos que han sido tratados.

Este lineamiento proporciona un marco práctico para realizar la anonimización de datos personales en cumplimiento de la Ley 1581 de 2012, incluyendo procesos aplicables a bases de datos electrónicas y manuales (físicas), con un enfoque en la protección efectiva de los derechos del titular.

2. OBJETIVO

Establecer las actividades y directrices para la Anonimización de la información sensible en las bases de datos de la Unidad que contienen datos sensibles y que son de la custodia de la UARIV, permitiendo así que se enmascare en el almacenamiento y la transmisión de acuerdo con la ley 1581 de 2012, política de protección de datos personales, y reducir al mínimo los riesgos de Re-identificación de los datos anonimizados.

3. DEFINICIONES

Acuerdo de Confidencialidad: Es un contrato legal entre al menos dos entidades para compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.

Anonimización¹: Es el proceso que impide la identificación de las unidades de estudio que son fuente para los registros individuales del conjunto de microdatos.

Datos íntimos o privados: Tienen como principal característica que pertenecen e interesan única y exclusivamente a la persona sobre la cual recae la información, razón por la cual solo pueden ser obtenidos en los siguientes casos:

- Con el consentimiento del titular de la información;
- Por orden de autoridad judicial en el cumplimiento de sus funciones;

¹ GUÍA DE ANONIMIZACIÓN DE DATOS ESTRUCTURADOS. Archivo general de la Nación Colombia. 2020. Disponible en internet URL: <[Guía de Anonimizacion-min.pdf](#)>

 Unidad para las Víctimas	LINEAMIENTO DE ANONIMIZACIÓN DE DATOS	Código: 140,06,16-13
	GESTION DE LA INFORMACION	Versión: 01
	PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACION	Fecha: 28/08/2025 Página 3 de 7

- Para salvaguardar la vida de la persona, cuando esta se encuentra en incapacidad física o jurídica;
- Cuando tengan una finalidad histórica, estadística o científica.

Ejemplo:

- Ideas y creencias religiosas.
- Orientación sexual.
- Afecciones a la salud.

Datos personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, protección de datos personales). Es toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento y transmisión, concerniente a personas físicas identificadas o identificables (tales como nombre, apellidos, estado civil, sexo, edad, domicilio, número de la seguridad social, número de matrícula del empleado, identificación personal, número de teléfono, etc.)

Datos públicos²: Son todos aquellos datos que conciernen a un interés general, tales como los documentos públicos, sentencias judiciales, los relativos al estado civil de las personas, entre otros.

Datos semiprivados: Estos datos, aun cuando tienen un carácter privado solo le interesan al titular y a un grupo determinado de personas, las cuales pueden consultar la información mediante una autorización. El ejemplo típico de esta clase de datos son las historias crediticias que administran las centrales de riesgo.

Datos sensibles: Información catalogada como pública clasificada o pública reservada. Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la 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 así como los datos relativos a la salud, a la vida sexual y los datos biométricos. (Ley 1581 de 2012, protección de datos personales).

Dato manual: Información registrada en medios físicos (archivos, formularios, registros en papel).

Enmascaramiento: Es un proceso que consiste en transformar los datos a partir de la aplicación de algoritmos de una sola vía, que permita a los sistemas procesar los datos, pero que a su vez no habilite a los usuarios finales a conocer los datos originales, los datos enmascarados deben conservar el mismo significado y sentido que los datos originales.

² GUÍA DE ANONIMIZACIÓN DE DATOS ESTRUCTURADOS. Archivo general de la Nación Colombia. 2020. Disponible en internet URL: <[Guía de Anonimizacion-min.pdf](#)>

 Unidad para las Víctimas	LINEAMIENTO DE ANONIMIZACIÓN DE DATOS	Código: 140,06,16-13
	GESTION DE LA INFORMACION	Versión: 01
	PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACION	Fecha: 28/08/2025 Página 4 de 7

Información pública: Es toda información que la entidad genere, obtenga, adquiera, o controle; corresponde a datos que son de acceso público y que por lo tanto no tienen requerimientos frente a la Confidencialidad. Está en esta clasificación la información denominada como “Pública” en la Ley 1712 de 2014 y como “dato público” en el decreto 1377 de 2013.

Información pública clasificada: Es aquella información que estando en poder o custodia de la entidad, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica 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. Esta corresponde a toda aquella información cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiere causar un daño a los siguientes derechos:

- El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado.
- El derecho de toda persona a la vida, la salud o la seguridad.
- Los secretos comerciales, industriales y profesionales.
- También corresponden a esta categoría los datos que son catalogados como “dato semiprivado o privado” de acuerdo con el decreto 1377 de 2013.

Información pública de Uso Interno: Es toda información que no contiene datos sensibles, que puede encontrarse en proceso de construcción, y que no requiere su divulgación a terceros, pero es necesaria para las actividades internas de la entidad.

Información pública reservada: Es aquella información que estando en poder o custodia de la entidad es exceptuada de acceso a la ciudadanía por daño a intereses públicos. Esta corresponde a aquella información cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito en las siguientes circunstancias, siempre que dicho acceso estuviese expresamente prohibido por una norma legal o constitucional:

- La defensa y seguridad nacional;
- La seguridad pública;
- Las relaciones internacionales;
- La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso;
- El debido proceso y la igualdad de las partes en los procesos judiciales;
- La administración efectiva de la justicia;
- Los derechos de la infancia y la adolescencia;
- La estabilidad macroeconómica y financiera del país;
- La salud pública;
- También corresponde a información de carácter reservado los datos catalogados como sensibles por el decreto 1377 de 2013.

 Unidad para las Víctimas	LINEAMIENTO DE ANONIMIZACIÓN DE DATOS	Código: 140,06,16-13
	GESTION DE LA INFORMACION	Versión: 01
	PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACION	Fecha: 28/08/2025 Página 5 de 7

Microdato: Son los datos sobre las características de las unidades de una población, (individuos, hogares, establecimientos, entre otros), que constituyen una unidad de información en una base de datos y que son recogidos por medio de una operación estadística.

Seudonimización³: Los datos son modificados, pero pueden ser revertidos. No es anonimización.

Re-identificación⁴: Se refiere a la identificación de los particulares a partir de un conjunto de datos que previamente fue des identificado o anonimizado.

Tratamiento de los datos personales: Hace referencia a cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

4. CRITERIOS

Los procesos de la entidad, a través de los colaboradores que se deleguen, deben revisar e identificar la información que debe ser anonimizada mínimo una vez al año de acuerdo con este lineamiento, e informar a la Oficina de Tecnologías de la Información (OTI) a través de correo electrónico, la cual vigila que los datos que están en su custodia o propiedad y que son catalogados como datos públicos, datos semiprivados, datos privados y datos sensibles se enmascaren al momento de almacenarse o transmitirse por cualquier medio. Toda anonimización debe respetar los principios de:

- Legalidad
- Finalidad
- Confidencialidad
- Seguridad
- Responsabilidad demostrada
- Conservación (solo por el tiempo necesario)

4.1 Anonimizar los datos

A la luz de la legislación existente (Ley 1581 de 2012 Disposiciones generales para la protección de datos personales, y Ley 1712 de 2014 Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones), se entiende la Anonimización como el resultado de un proceso de tratamiento de los datos, con el fin de evitar la identificación de una persona de manera directa o indirecta y de forma irreversible. Este proceso controla el riesgo de identificación de las personas que acceden a entregar su información con datos personales, según los medios disponibles, teniendo en cuenta que se debe preservar la utilidad y aprovechamiento de los datos que necesitan los funcionarios,

³ GUÍA DE ANONIMIZACIÓN DE DATOS ESTRUCTURADOS. Archivo general de la Nación Colombia. 2020. Disponible en internet URL: <[Guía de Anonimizacion-min.pdf](#)>

⁴ La Anonimización: Conceptos y Procesos. Blog de delegado de Protección de Datos. 2023. Disponible en internet URL: < [La anonimización; Conceptos y procesos - Delegado de protección de datos](#)>

 Unidad para las Víctimas	LINEAMIENTO DE ANONIMIZACIÓN DE DATOS	Código: 140,06,16-13
	GESTION DE LA INFORMACION	Versión: 01
	PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACION	Fecha: 28/08/2025 Página 6 de 7

contratistas o proveedores. Estos datos pueden estar contenidos en tablas de resumen de información, gráficos y demás documentos y publicaciones derivadas del que hacer estadístico; en estos casos el análisis o desagregación de la información de manera muy detallada, puede revelar información sensible o confidencial que conlleve a la identificación de una persona en particular.

La entidad a través de la OTI vigila los datos que están en su custodia o propiedad y que son catalogados como datos públicos, datos semiprivados, datos privados y datos sensibles se enmascaren al momento de almacenarse o transmitirse por cualquier medio.

La entidad, como responsable de la información, cuenta con avisos de privacidad y autorización por parte de los titulares de la información, para la recolección, almacenamiento, uso, circulación y supresión de la información. Así mismo se establece el principio de responsabilidad demostrada como responsables del tratamiento de datos personales en donde implementa medidas efectivas y pertinentes para cumplir con las obligaciones establecidas en la Ley 1581 de 2012.

La ley no establece mecanismos o instrumentos para la protección de la información. Por ello, las herramientas o metodologías utilizadas para llevar a cabo la Anonimización de un conjunto de datos deben ser constantemente evaluadas y actualizadas según la tecnología disponible y los elementos contextuales, teniendo en cuenta que este proceso lleva implícito un factor de riesgo. Adicional, todos los funcionarios, contratistas o proveedores que manejen, procesen o reciban información de la entidad a través de los diferentes sistemas de información o aplicaciones y que de forma directa manipulan los datos (incluyendo información considerada estrictamente confidencial) referentes a la edad, procedencia, salud, raza, religión, ideología, etc., y que requieren de una protección especial deberán informar a la OTI mediante correo electrónico, que esa información sensible puede ser manejada con fines inapropiados generando una reducción en la confianza de quienes entregan información a la Entidad y afectando extensamente la credibilidad de la misma; una vez realizado el reporte, la OTI procederá a la custodia y medidas de Anonimización que se tienen adoptadas en la entidad.

4.2 Métodos para realizar anonimización en la entidad:

- Para datos electrónicos:
 - Supresión directa: Eliminar o reemplazar nombres, cédulas, direcciones.
 - Generalización: Reemplazar valores con rangos. Ej: Edad → 30-40.
 - Perturbación: Agregar ruido a los datos numéricos.
 - Encriptación irreversible (hash sin clave): Codificar sin posibilidad de decodificación.
 - Agregación: Unir datos individuales en grupos. Ej: promedio salarial por ciudad.
- Para datos físicos (manuales):
 - Tachado irreversible de campos identificadores: Usar marcadores permanentes o destrucción física controlada.
 - Digitalización sin elementos identificadores: Escanear documentos tras borrar o cubrir datos personales.

 Unidad para las Víctimas	LINEAMIENTO DE ANONIMIZACIÓN DE DATOS	Código: 140,06,16-13
	GESTION DE LA INFORMACION	Versión: 01
	PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACION	Fecha: 28/08/2025 Página 7 de 7

- Fragmentación de documentos: Separar o destruir hojas que contengan datos sensibles.
- Recodificación manual: Sustituir nombres por códigos que no tengan relación con la identidad.
- Uso de etiquetas neutras: En formularios antiguos, sustituir referencias personales por símbolos genéricos.

4.3 Evidencias que se deben cumplir al realizar anonimización de datos.

Cada anonimización debe incluir:

- Fecha y responsables.
- Datos y campos tratados.
- Método aplicado y justificación.
- Resultado de evaluación de reidentificación.
- Firma del DPO y responsable.

4.3.1 Verificación y validación.

Antes de declarar datos como anonimizados:

- Validar que no existan datos directos o indirectos.
- Simular intentos de reidentificación.
- Revisar cumplimiento de principios de la Ley 1581.

4.3.2 Conservación y destrucción.

- Los datos anonimizados pueden conservarse para fines estadísticos o investigativos.
- Si los datos ya no tienen utilidad, se deben destruir de forma segura.

5. DOCUMENTOS DE REFERENCIA

- Resolución 03157 de 2021, establece la política general del Sistema de Gestión de Seguridad de la Información y sus políticas específicas.
- Guía de Anonimización de Datos Estructurados del archivo general de la nación.

6. ANEXOS

No aplica.

7. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	28/08/2025	Creación del documento