Guía

de disociación, anonimización y seudonimización

de datos personales para entidades públicas

PERÚ | Ministerio de Justicia y Derechos Humanos

Guía de disociación, anonimización y seudonimización de datos personales para entidades públicas

Autoridad Nacional de Protección de Datos Personales
Octubre 2025

Calle Scipión Llona 350, Miraflores, Lima – Perú
Teléfono: 204 8020 anexo 2410
https://www.gob.pe/minjus
E-mail: protegetusdatos@minjus.gob.pe

Ministro de Justicia y Derechos Humanos:
Walter Eleodoro Martínez Laura

Viceministro de Justicia:
Jesús Adalberto Baldeón Vásquez

Director General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales:
Eduardo Luna Cervantes

Directora de Protección de Datos Personales:
María Alejandra González Luna

Directora de Fiscalización e Instrucción
Olga Escudero Vílchez

Directora de Transparencia y Acceso a la Información Pública:
Marcia Águila Salazar

Elaboración, revisión y edición:

Esta Guía ha sido elaborada por un equipo mixto de las direcciones de línea que integran esta Dirección General y revisado por las directoras y director de las mismas. Responsables de edición, Sandra Amelia Flores Ramos, Especialista Legal, y Víctor Fernando Calderón Valladares, Analista de fiscalización en seguridad de la información.

1.ª edición octubre de 2025
Hecho el Depósito Legal en la Biblioteca Nacional del Perú N.º 2025-12172

Presentación

¿Por qué disociar, anonimizar y seudonimizar datos personales de documentos físicos o digitales? Una respuesta corta nos obligaría a responder con otra pregunta, ¿y por qué no? Y es que la carga de justificar que un dato personal deba ser tratado para diversos fines públicos radica en quien tiene ese poder público que los determina; pues el dato personal no es de la entidad que lo trata, sino de la persona humana.

Si la carga de la prueba para justificar el tratamiento de datos personales está en quien asume la responsabilidad de tratarlos por el poder público que ejerce, hay algunas formas de hacerlo y no morir en el intento. Una primera es hacer descansar esa legitimidad para el tratamiento de datos que se efectúa en la Ley. En efecto, si una ley determina que cierta entidad pública debe hacer un tratamiento de datos personales (recabarlos, almacenarlos, transmitirlos, procesarlos, etc.) se acabó la discusión, porque para eso están las leyes –como dirían los ilustres profesores y filósofos del derecho de la Universidad de Alicante, Manuel Atienza y Juan Ruiz Manero–, para exponernos razones para la acción de carácter perentorio (se debe realizar la acción exigida por ella misma por tratarse de una norma legítimamente emitida por quien tiene el poder legitimado para hacerlo) e independientes de contenido (porque excluyen cualquier deliberación del destinatario de la norma).

Así que, si una entidad pública tiene, por ejemplo, que recabar datos referidos a nuestra intimidad económica para cumplir con su mandato legal, verbigracia, la Superintendencia Nacional de Aduanas y de Administración Tributaria (Sunat), pues puede hacerlo. Sin más trámite y miramientos, pero sólo para esa finalidad determinada por la ley; entiéndase, en este caso, conocer nuestro patrimonio y, en función de nuestra renta y capacidad contributiva, supervisar el pago de nuestros impuestos.

Pero hay situaciones en las que justificar determinado tratamiento de datos personales en la ley no es tan claro porque no hay una alusión expresa a ellos. Para ser más precisos, la alusión es a las funciones y competencias que deben realizar entidades públicas y que presuponen la gestión de documentos, físicos y digitales donde yacen los datos personales, pero no expresa ni directamente a estos últimos.

Un buen ejemplo es la función (vista la obligación) de toda entidad pública de atender solicitudes de acceso a la información pública, a propósito del ejercicio del derecho fundamental de acceso a la información pública (artículo 2.5 de la Constitución) y de las obligaciones de la Ley de Transparencia y Acceso a la Información Pública (Ley N.º 27806). Un documento que esencialmente es de naturaleza pública, puede albergar información no pública, como es el caso de los datos personales que supongan una afectación a la intimidad personal (artículo 17.5 de la Ley N.º 27806 – Texto Único Ordenado). Siendo así, ¿qué debe hacerse entonces para

satisfacer óptimamente ambos derechos contrapuestos? Reproducir y entregar la información de manera disociada y/o anonimizada, es decir, una atención parcial de la solicitud (artículo 19 del TUO de la Ley N.º 27806). ¿Cómo segregar la información? Para eso sirven las técnicas de disociación y anonimización que esta Guía presenta.

Otro ejemplo es la función (vista la obligación) de las entidades públicas del sistema de justicia de publicar sentencias, dictámenes fiscales y, en general, jurisprudencia sistematizada, en sus portales de transparencia (artículo 39 del citado TUO). ¿Cómo debe cumplirse esta obligación sabiendo que existen otras que determinan el resguardo de la identidad de la persona? Por ejemplo, en los procesos penales por delitos contra la libertad sexual (literal c) del artículo 95 del Nuevo Código Procesal Penal, Decreto Legislativo N.° 957) o cuando un fiscal disponga medidas de reserva de identidad en las diligencias que se practiquen (literal d) del numeral 2 del artículo 248 del NCPP). En el cumplimiento de este tipo de obligaciones es que se enmarca la Guía que se presenta y las técnicas de disociación y anonimización que contiene.

Y es que, cómo debemos entender el llamado principio de la privacidad desde el diseño y por defecto (numeral 5.3 del artículo 5 de la Ley de Gobierno Digital, aprobada por el Decreto Legislativo N° 1412) si no es asumiendo la idea de que el dato personal no le pertenece a la administración estatal por el mero hecho de poseerlo. El dato personal es, al fin y al cabo, una expresión o manifestación de la individualidad de la persona y no es un activo de la organización para usos diversos y convenientes para la gestión; ni aun alegando interés o beneficio para el titular del mismo, sin mediar su consentimiento.

Si desde el diseño y configuración de servicios digitales deben adoptarse medidas preventivas de tipo tecnológico, organizacional, humano y procedimental para preservar la privacidad, entonces eso significa que deben agotarse todas las acciones encaminadas para proteger los datos personales, pues es en la autodeterminación del titular de los mismos donde se establece el umbral de lo que quiere hacerse público –y lo que no– en resguardo de la privacidad. Y eso pasa por evitar que, por ejemplo, cuando se consume un servicio digital para el llenado de un formulario de Libro de Reclamaciones se autocomplete automáticamente en él todos los datos personales del reclamante, sólo por haber digitado antes –y únicamente– su documento nacional de identidad, exponiendo así una serie de datos que contiene el DNI para cualquiera que tenga a mano un número de documento de identidad de cualquier persona; pasa también, por conjurar situaciones que hagan visibles datos personales de un individuo al no gestionar ex ante la no indexación –por parte de motores de búsqueda– de la página web que contiene el documento o recurso donde yacen estos; o, pasa, por último, cuando no se adoptan las medidas de seguridad que corresponden (encriptación, por ejemplo) para almacenar información personal sensible.

En suma, asumir por regla general que la privacidad es la que impera, y que el dato personal no es de libre disposición de quien lo posee, sino de su titular, es la razón para que la administración estatal se familiarice con técnicas de disociación, anonimización y seudonimización de datos personales y las aplique en documentos físicos o digitales, sea para cumplir con alguna obligación jurídica que derive de una regla expresa o sea para cumplir con una obligación jurídica que, en su ejecución, tiene también que observar principios como el de privacidad desde el diseño y por defecto o el principio de proporcionalidad (artículo 7 de la Ley N.º 29733).

La Guía que se presenta consta de siete (7) secciones y un anexo con el listado de las opiniones consultivas e informes jurídicos de la Autoridad Nacional de Protección de Datos Personales más relevantes sobre la temática de interés, antecedidos por un epígrafe de Siglas y abreviaturas y un Glosario de términos. La primera y segunda sección abordan conceptos y nociones básicas como el dato personal, la disociación, anonimización y seudonimización de datos personales. La tercera presenta una nota explicativa acerca de los escenarios de aplicación de estas técnicas y de las razones de importancia para hacerlo. La cuarta sección está dedicada a los criterios de minimización de datos y de privacidad desde el diseño y por defecto, que deben considerarse ex ante en los procedimientos de disociación, anonimización y seudonimización de datos personales. La quinta, a los pasos básicos a seguir para aplicar eficientemente estos procedimientos. La Guía concluye con las secciones sexta y séptima, dedicadas específicamente a las técnicas recomendadas para la entrega y/o publicación de información que contiene datos personales y la técnica de seudonimización, como la más común empleada para la conservación y almacenamiento de información de datos personales.

El Ministerio de Justicia y Derechos Humanos, a través de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, que ejerce la Autoridad Nacional de Protección de Datos Personales, presenta pues esta Guía de elaboración propia. Y lo hace con el ánimo de facilitar y promover la protección de datos personales en el quehacer cotidiano de las administraciones públicas, a propósito de la gestión documentaria que realizan y las obligaciones a cumplir derivadas de ella.

Lima, octubre de 2025

Eduardo Luna Cervantes
Director General
Dirección General de Transparencia,
Acceso a la Información Pública
y Protección de Datos Personales

Índice

Siglas y abreviaturas

ANPD	AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES
ANTAIP	AUTORIDAD NACIONAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA
DGTAIPD	DIRECCIÓN GENERAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES
DL	DECRETO LEGISLATIVO
DS	DECRETO SUPREMO
LPDP	LEY DE PROTECCIÓN DE DATOS PERSONALES
LTAIP	LEY DE TRANSPARENCIA Y ACCESO Y A LA INFORMACIÓN PÚBLICA
RLPDP	REGLAMENTO DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES
TUO	TEXTO ÚNICO ORDENADO

Glosario de términos

Para la presente guía se consideran las siguientes definiciones:

1. **Anonimización:** Procedimiento en virtud del cual se realiza un tratamiento de datos personales con fines de impedir la identificación del titular de los mismos. Es irreversible por la imposibilidad de reidentificar al titular de los datos personales, cualquiera sea el formato (físico o digital) empleado para su entrega y/ o publicación.

   Para efectos de esta Guía, la aplicación de la anonimización se realiza sobre la copia del documento que contiene los datos personales del titular y se puede realizar tanto en formatos digitales como en formatos físicos[1] respecto a datos estructurados, no estructurados y semiestructurados.

   El documento anonimizado puede ser reutilizado o difundido sin comprometer la privacidad ni los derechos del titular de los datos personales, por lo que, se advierte que el resultado del procedimiento de anonimización deja de estar comprendido en el ámbito de aplicación de la Ley de Protección de Datos Personales y su reglamento.

   La aplicación de este procedimiento, requiere de una revisión periódica con el objeto de asegurar que, a través del tiempo, se continue garantizando la reducción de posibilidad de reidentificación del titular.

2. **Atributo de datos:** Es una característica o propiedad específica de un dato dentro de un conjunto de datos que lo define como tal.

3. **Banco de datos personales.** Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

4. **Datos estructurados:** Son datos que se encuentran en un formato específico, estandarizado y estructurado para almacenar y organizar determinada información permitiendo que la identificación, búsqueda y tratamiento de información sea sistematizada. Dichos datos se pueden encontrar, entre otros, en bases de datos y hojas de cálculo.

   Los datos estructurados solo podrán existir en formatos digitales (ej. hoja Excel, archivos XML, SQL, etc.).

1 Cuando la única opción disponible para entregar el documento es una copia física la técnica de anonimización queda limitada solo a la técnica del tachado.

5. **Datos no estructurados:** Son datos que no presentan una estructura específica ni se ajustan a un modelo de datos o formato; asimismo, su tratamiento es mucho más complejo y requiere de un análisis y aplicación particular de las técnicas disponibles para ser analizados y procesados.

   Los datos no estructurados pueden existir en formatos digitales (ej. documentos de texto Word, PDF[2], documentos escaneados, chats, audios, videos, etc.) y en formatos físicos (ej. documentos impresos, fotografías, cartas, resoluciones, etc.)[3].

6. **Dato personal:** Es toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

7. **Datos personales relacionados con la salud:** Es aquella información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo la información que se derive de un acto médico, el grado de discapacidad y su información genética.

8. **Datos semiestructurados:** Son datos que no tienen una estructura fija (como una base de datos); no obstante, la manera como se encuentra organizada la información contenida en el documento permite identificar, entender los tipos de datos y, hasta cierto punto, sistematizarlos.

   Los datos semiestructurados pueden encontrarse en archivos en formato XML, correos electrónicos (campos definidos "De", "Para", "Asunto", pero el contenido del cuerpo es libre), archivos HTML, etc.

   Si bien los documentos en formatos PDF y Word se consideran datos no estructurados, dichos archivos pueden también ser datos semiestructurados, en la medida que cuenten con determinadas estructuras reconocibles y sistemáticas (campos fijos, tablas, formularios, entre otros) por lo que el archivo deja de ser libre y puede procesar de forma parcial información de manera automatizada. Respecto a un documento con formato PDF o Word este puede tener un formulario o tablas con campos definidos (nombre, Documento Nacional de Identidad, fecha de nacimiento).

9. **Dato sensible:** Es aquella información relativa a datos genéticos o biométricos de la persona natural, datos neuronales, datos morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la afiliación sindical, salud física o mental u otras análogas que afecten su intimidad.

2 Aunque el dato o algún texto se pueda identificar a través de una búsqueda nominal (porque es un PDF que permite su lectura y no una imagen escaneada), su contenido no está organizado para ser procesado sistemáticamente por una máquina sin interpretación previa, por lo cual, en este caso, la naturaleza del formato PDF corresponde a un dato no estructurado.

3 Mientras mantengan una estructura específica, siguen siendo datos no estructurados, aunque no puedan ser procesados automáticamente sin digitalización.

10. **Disociación:** Procedimiento en virtud del cual se realiza un tratamiento de datos personales con fines de impedir la identificación del titular de los mismos o de un atributo o cualidad de él que lo haga identificable, mientras se mantiene cierto nivel de información sobre el mismo. Es reversible por la posibilidad de reidentificar al titular de los datos personales, en tanto aún se conserva cierto atributo o propiedad el dato personal.

    La aplicación de disociación de datos personales se puede realizar tanto en formatos digitales como en formatos físicos; no obstante, debido a la naturaleza del procedimiento, este, en la mayoría de casos, es aplicable para datos estructurados. Sin perjuicio de ello, al existir limitaciones a través de otros formatos las técnicas de disociación también se pueden aplicar para datos no estructurados y semiestructurados.

    Para evitar la reidentificación del titular de los datos personales es recomendable realizar más de una técnica de disociación.

11. **Documento:** Es aquel soporte (físico o digital) que contiene información (textual y no textual) que contiene datos en cualquier formato (estructurado, no estructurado y semiestructurado) y que ha sido producida, recibida o almacenada para el cumplimiento de determinada finalidad y que, de corresponder, puede servir como evidencia, constancia o respaldo de actos, decisiones o procedimientos.

    Es preciso mencionar que, información textual versa sobre un lenguaje escrito, esto es, oficios, cartas, informes, resoluciones, correos electrónicos, libros, normas, archivos de texto digital (PDF, Word, TXT, etc.); mientras que, la información no textual, puede expresarse en medios gráficos, visuales, auditivos, entre otros, como escaneo de documentos (sin OCR), imágenes, fotografías, videos, grabaciones, esquemas, formatos digitales multimedia, etc.

12. **Documento entregable de información:** Es el formato (ya sea físico o digital) que contiene la información del titular de los datos personales, destinado al acceso público en el que se le puede aplicar un procedimiento de disociación o anonimización.

13. **Encargado del tratamiento de datos personales:** Es la persona natural, persona jurídica de derecho privado o entidad pública que realiza tratamiento de datos por cuenta u orden del responsable de tratamiento o titular del banco de datos personales.

14. **Enfoque de riesgo:** Enfoque a través del cual se emplean métodos o estrategias que permiten identificar, evaluar y gestionar los riesgos a suscitar que pueden afectar el tratamiento de datos personales con el fin de implementar medidas de mitigación o prevención, siendo por tanto la evaluación de impacto en la protección de datos personales una herramienta clave para su aplicación.

15. **Entidad pública.** Entidad comprendida en el artículo I del Título Preliminar de la Ley N.° 27444, Ley del Procedimiento Administrativo General.

16. **Hipervisibilidad:** Situación en la cual los datos personales de un titular o de varios son expuestos en entornos físicos o digitales de tal manera que se magnifique su difusión por el medio empleado y/o por la prolongación del tiempo de exposición.

    La hipervisibilidad de datos personales puede darse con prescindencia de la intención o consentimiento del titular de los mismos o de la legitimidad de la fuente informativa que la genera o del grado de accesibilidad o reutilización de los datos expuestos. La hipervisibilidad puede generar un riesgo de estigmatización o discriminación del titular de los datos personales.

17. **Identificadores:** Son datos que por sí solos o en combinación con otros datos permiten identificar o reconocer a una persona. Ejemplos de identificadores pueden ser: nombre y apellidos, DNI, correo electrónico o ubicación geográfica. Se usan para poder realizar perfilamiento, vigilancia de datos, entre otros.

18. **Principio de minimización de datos personales:** El responsable de los datos personales procurará realizar esfuerzos razonables para tratar los datos personales al mínimo necesario, con relación a las finalidades que motivan su tratamiento y para evitar la reidentificación del titular de los datos personales.

19. **Reidentificación:** Procedimiento empleado con fines de identificar a un titular de datos personales, cuyos datos personales fueron previamente sometidos a un procedimiento de disociación, anonimización y seudonimización.

20. **Responsable del tratamiento de datos personales:** Es la persona natural, persona jurídica de derecho privado o entidad pública que decide sobre la finalidad y medios del tratamiento de datos personales. Esta definición no se restringe al titular del banco de datos, sino que incluye a cualquier persona que decida sobre el tratamiento de datos personales, aun cuando no se encuentre en un banco de datos personales.

21. **Repertorio de jurisprudencia:** Es la compilación sistemática y ordenada de decisiones jurídicas relevantes (resoluciones administrativas, sentencias judiciales, laudos arbitrales, opiniones vinculantes, dictámenes fiscales, jurisprudencia internacional relevante, resoluciones de consejos de ética de colegios profesionales, de universidades, entre otros) elaboradas por entidades públicas o privadas que se encuentran destinadas al conocimiento público y que sirven, principalmente, como fuente de consulta, análisis u orientación interpretativa de normas jurídicas o deontológicas, principalmente.

22. **Seudonimización:** Es una técnica para procesar datos personales sustituyendo identificadores por seudónimos, haciendo imposible identificar a una persona sin información adicional.

Para efectos de esta guía, respecto al almacenamiento, conservación y tránsito de datos, se considerará la técnica de la seudonimización por aplicación de algoritmos de cifrado bidireccional (permiten la reversibilidad del dato cifrado) y por aplicación de una función criptográfica HASH (no permite la reversibilidad del código generado).

La seudonimización por aplicación de algoritmos de cifrado bidireccional, es un procedimiento reversible que permite la conservación, almacenamiento y tránsito seguro de datos personales en contextos informáticos. En este proceso, los datos se transforman en un texto ininteligible incluso para la propia entidad titular de la base de datos, de modo que solo pueden ser tratados o restituidos a su forma original mediante el uso de una llave de cifrado integrada en los sistemas de información correspondientes.

La seudonimización mediante una función criptográfica hash es un procedimiento irreversible que transforma un dato personal en un código único (código hash), el cual puede utilizarse para verificar la integridad del dato original. Sin embargo, a pesar de esta irreversibilidad, en determinados escenarios podría ser posible reidentificar al titular del dato si el código hash se combina con información adicional que permita inferir cuál era el dato personal inicial.

En ese sentido, los datos seudonimizados, aun cuando se encuentren en un formato codificado reversible o irreversible, conservan su carácter de datos personales y, en consecuencia, deben ser tratados conforme a los principios y obligaciones legales previstos en la LPDP y su Reglamento (tales como los principios de seguridad, finalidad, proporcionalidad y consentimiento) cuya observancia resulta indispensable para garantizar en todo momento la protección efectiva de los derechos de los titulares.

23. **Software:** Es un componente intangible formado por un conjunto de programas, datos, instrucciones, entre otros, que permite realizar tareas específicas en un sistema informático.

24. **Titular de datos personales:** Persona natural a quien le corresponden los datos personales.

25. **Titular del banco de datos personales:** Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

26. **Tratamiento de datos personales:** Es cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales o sensibles.

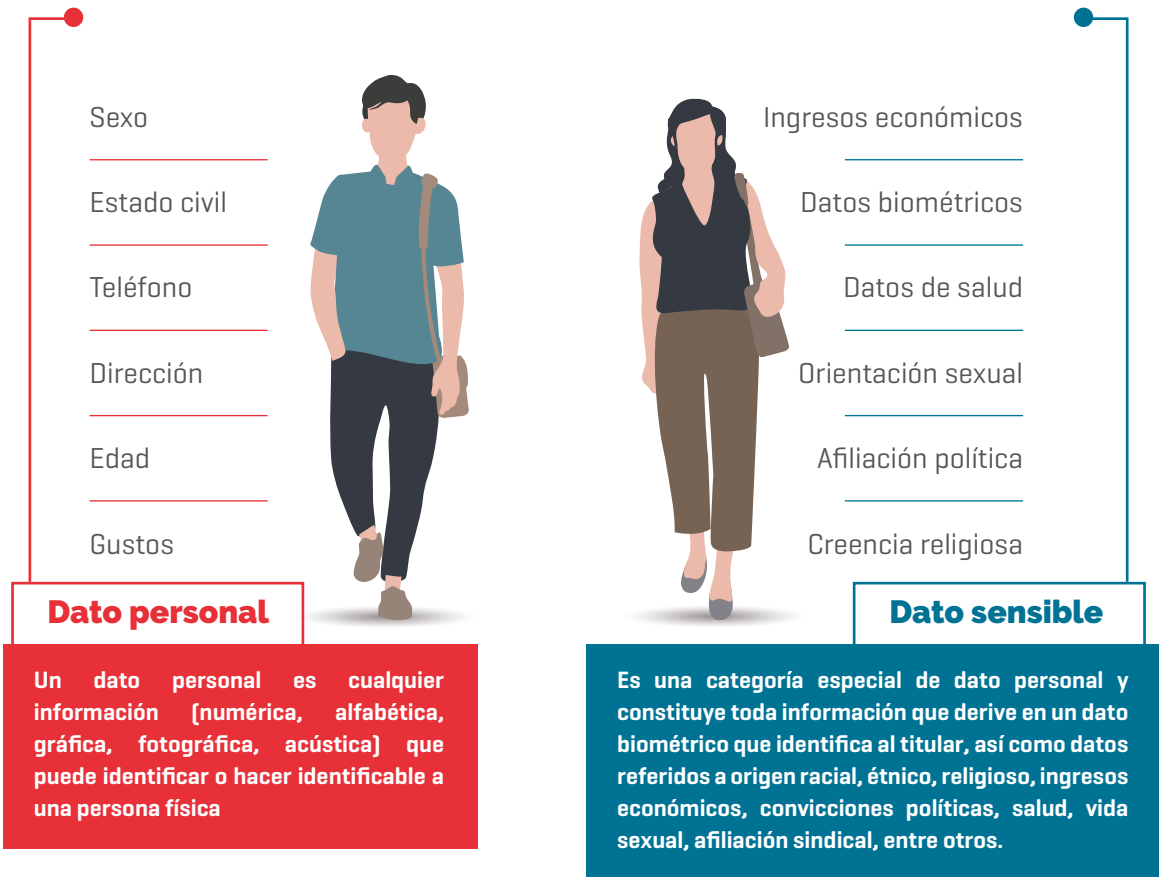
1

Datos personales objeto de disociación, anonimización y seudonimización

1 Datos personales objeto de disociación, anonimización y seudonimización

Para la aplicación de las técnicas de disociación, anonimización y seudonimización que se detallan más adelante, es necesario tomar en cuenta el concepto de dato personal y sus componentes, y así advertir qué información podría reidentificar al titular de los datos personales a propósito del tratamiento que se practique sobre los mismos.

Al respecto, según lo establecido en la LPDP y en su RLPDP, es necesario recordar:



Nota

Para poder realizar el procedimiento de disociación, anonimización y seudonimización de datos personales, resulta necesario que se puedan identificar los componentes principales de los datos personales.

Al respecto, se define como componentes de los datos personales a aquella(s) característica(s) que permite(n) identificar, sea directa o indirectamente, a una persona.

Componentes directos

Es la información que identifica y distingue a una persona natural dentro de un grupo de personas.

- Nombres o apellidos
- Dirección de correo electrónico
- Número de celular
- N.º de DNI, N.º de pasaporte
- Imagen y voz
- Firma
- Nombre de usuario en redes sociales, entre otros.

Componentes indirectos

Es la información no exclusiva de un individuo, que en principio no permite reconocer a la persona natural, sin embargo, puede ser identificable si se combina con otros datos, tales como las características físicas, psíquicas, económicas, culturales o sociales.

- Edad, altura o peso
- Género
- Estado civil
- Carrera profesional
- Fecha de nacimiento
- Dirección
- Dirección IP, URLs, ubicación de GPS, entre otros.

Nota

El reconocimiento de la información que identifica o permite identificar a un individuo con la asociación de otros datos permite a la entidad aplicar las técnicas adecuadas que minimicen los riesgos de reidentificación de los titulares de los datos personales.

Ejemplo

La entidad judicial de una comunidad habitada por sesenta (60) personas publica en su portal de transparencia un resumen de resoluciones judiciales referidas a casos de violencia familiar en su jurisdicción, entre los cuales, uno versa sobre un proceso por maltrato infantil. Si bien en la mencionada resolución se omite el nombre del menor de edad, se consignan los nombres de los padres de familia, conforme al siguiente extracto:

Extracto de la resolución judicial:

> *"La señora Teodora Churata Vilca denuncia al señor Juan Zárate Huanca por agresiones físicas y psicológicas contra su menor hijo en el domicilio ubicado en la comunidad de la Amistad (distrito de San Datito), solicitando medidas de protección a favor del niño."*

Considerando que la comunidad tiene pocos habitantes, aunque el nombre del menor de edad no fue publicado en la resolución judicial, su identificación sí es posible en la medida que se han difundido los datos de sus padres, por lo que dicha situación generaría una vulneración al derecho de la protección de los datos personales del menor de edad, al no garantizar su anonimato.

Por tanto, este caso exige que se apliquen las técnicas de disociación y anonimización más convenientes para el resguardo del derecho a la intimidad del menor, evitando de esta manera su exposición.

2

Nociones preliminares sobre disociación, anonimización y seudonimización

2 Nociones preliminares sobre disociación, anonimización y seudonimización

2.1. Alcances

Para la presente guía, la selección y aplicación de las técnicas de disociación, anonimización[4] y seudonimización dependen de la finalidad particular de la entrega y/o publicación[5] de la información y de la compatibilidad con el formato de origen de los datos (estructurados, no estructurados y semiestructurados). Por ejemplo, mientras que la entrega y/o publicación de datos estructurados (bases de datos), permite a la entidad la aplicación de múltiples técnicas de disociación, la entrega y/o publicación de información que contiene datos semiestructurados o no estructurados (copias de informes, resoluciones, cartas, entre otros) limita tal aplicación.

Asimismo, la documentación original siempre se mantendrá en custodia de la entidad pública encargada del tratamiento de los datos personales del titular, siendo que la copia en formato físico o digital sobre la cual se aplique el procedimiento de disociación y anonimización será la que finalmente se entregue y/o publique (documento entregable de información).

Para fines de la presente guía, el procedimiento de seudonimización se limitará a la aplicación de algoritmos de encriptación bidireccional, los que se encuentran diseñados para permitir el almacenamiento y tránsito seguro de información y mantienen como característica principal su reversibilidad. Esta debe entenderse en un contexto enteramente virtual, donde son los sistemas de información los que requieren acceder, en entornos seguros, a estos datos; poder leerlos, por ejemplo, y volver a encriptarlos, por lo que los datos personales seudonimizados por encriptación se encuentran sujetos al cumplimiento de la LPDP y su RLPDP. Los algoritmos de encriptación bidireccional brindan seguridad, entre otros, al envío de correos electrónicos, transacciones bancarias, llamadas telefónicas, entre otros.

Por otro lado, respecto a la seudonimización, la guía también se ocupa de la función criptográfica unidireccional hash, la cual construye un código único a partir de un dato, y que, si bien no permite reconstruir el dato original a partir del código generado (código hash), es posible "dar" con el dato original, en el escenario tecnológico adecuado, a través de comparaciones masivas u otras técnicas de contraste automatizado.

4 La aplicación de técnicas en la disociación y anonimización resultan relevantes en, entre otros, escenarios donde la información a entregar y/o publicar forma parte de bases documentales y de repertorios de jurisprudencia.

5 A efectos de la presente guía el procedimiento de seudonimización solo se aplicará para el tratamiento de datos personales relacionado a la conservación, almacenamiento y tránsito seguro de información en custodia de la entidad pública y al intercambio seguro de información para validación de dichos datos, siempre que la entidad lo considere pertinente; por lo cual la entrega y/o publicación de datos personales por sí mismo no se aplicaría en este caso.

Es importante señalar que, los procedimientos de disociación y anonimización comparten la misma finalidad: reducir al máximo el riesgo de reidentificación del titular de los datos personales al momento de la entrega y/o publicación de información que los contiene; escenario distinto al procedimiento de seudonimización, cuya finalidad difiere de la primera en tanto se aplica principalmente para el almacenamiento, conservación y tránsito seguro de la información (bases de datos).

2.2. Disociación

La disociación es un procedimiento que tiene como objetivo reducir al máximo el riesgo de reidentificación del titular de los datos personales mientras se mantiene determinado nivel de información sobre el mismo. Si bien la LPDP define la disociación como reversible, esto no implica la reconstrucción directa ni automática del dato personal original, más bien, supone que el dato disociado conserva determinados atributos o fragmentos de información que, en escenarios específicos y mediante el cruce con otras fuentes o técnicas avanzadas, podrían facilitar la reidentificación.

En este sentido, aunque la disociación mantiene un riesgo latente de vinculación, su finalidad es precisamente impedir la reidentificación directa y razonable del titular de los datos personales, al igual que la anonimización, garantizando que el tratamiento preserve cierta utilidad sin exponer de manera inmediata la identidad.

- **Disociación de datos personales en soportes físicos o no automatizados**
  En caso se requiere entregar una copia de un documento original en formato físico, el universo de técnicas de disociación disponibles se reduce de acuerdo a las limitaciones que suponen dichos documentos, lo que restringe la aplicación de técnicas de naturaleza digital, quedando únicamente disponibles aquellas compatibles con los formatos impresos, por lo que no se recomienda realizarla salvo que sea la única opción disponible, quedando a consideración de la entidad si en su lugar conviene la aplicación de un procedimiento de anonimización.

- **Disociación de datos personales en soportes digitales o automatizados**
  Respecto a la información digital que será materia de entrega y/o publicación por la propia entidad hacia terceros o para conocimiento público, se recomienda la aplicación de múltiples técnicas de disociación de datos personales que deben de organizarse de acuerdo al nivel de riesgo de reidentificación, de manera que el resultado no pueda reidentificar de manera inmediata y razonable al titular de los datos personales.

  La aplicación de técnicas de disociación de datos personales en documentación digital se tiene que realizar siempre respecto a un formato compatible, esto es, información que puede ser modificada, actualizada, corregida o eliminada a través de medios digitales (sistemas de información, herramientas, software especializado).

2.3. Anonimización

El procedimiento de anonimización es irreversible por la imposibilidad de reidentificar al titular de los datos personales. Esta irreversibilidad tiene como objetivo suprimir, al momento de su aplicación, toda posibilidad razonable de reidentificación del titular. Sin embargo, aún la anonimización puede conllevar un riesgo residual en escenarios altamente sofisticados, aunque en un grado mucho menor que en la disociación.

Por tanto, la entidad pública encargada del tratamiento de los datos personales de su titular y que realiza el procedimiento de anonimización debe gestionar los riesgos de una posible reidentificación adoptando filtros idóneos y una mejora continua sobre las técnicas de anonimización a usar.

En ese sentido, la anonimización hay que considerarla como un proceso basado en el **enfoque de riesgo,** para el cual resulta necesario evaluar la aplicación de técnicas disponibles al universo de datos o documentos a anonimizar.

A modo de resumen, a continuación, el detalle de las principales características de la disociación y anonimización:

CARACTERÍSTICAS	DISOCIACIÓN	ANONIMIZACIÓN
Datos estructurados	Aplicable	Aplicable
Datos no estructurados	Aplicable, con las restricciones que implique el documento o la información no estructurada.	Aplicable, con las restricciones que implique el documento o la información no estructurada.
Datos semiestructurados	Aplicable, con las restricciones que implique el documento o la información semiestructurada.	Aplicable, con las restricciones que implique el documento o la información semiestructurada.
Procedimiento	Reversible, en tanto el dato no desaparece, sino que pierde precisión.	Irreversible bajo toda razonabilidad*
Finalidad	Entregar y/o publicar datos personales que conserven cierto valor informativo reduciendo al máximo la posibilidad de reidentificación	Entregar y/o publicar datos personales, eliminando totalmente (razonablemente) el(los) dato(s) personal(es) y reducir al máximo la posibilidad de reidentificación

*La irreversibilidad del procedimiento debe ser total al momento en que se realiza dicho procedimiento, no obstante, es imposible asegurar la no reidentificación del titular en el futuro, ello en la medida que la aparición de nuevos datos o nuevas tecnologías pueden permitir la reidentificación del titular de los datos personales, por lo cual, se deben de adoptar medidas y actualizar la(s) técnica(s) para evitar dicho escenario.

2.4. Seudonimización

Para efectos de la presente guía, la seudonimización comprende la aplicación de algoritmos de cifrado bidireccional sobre datos personales, de modo que estos se almacenen en una base de datos en forma de texto ilegible (cifrados) para terceros no autorizados. En este escenario, los sistemas de información que acceden a dichas bases de datos requieren disponer de la llave de cifrado correspondiente, a fin de revertir los datos a su forma original y permitir su tratamiento legítimo, tras lo cual deben ser nuevamente cifrados antes de su almacenamiento. En consecuencia, los datos personales seudonimizados mediante técnicas de encriptación continúan siendo considerados datos personales y, por tanto, se encuentran sujetos al cumplimiento de la LPDP y el RLPDP.

Asimismo, se considera dentro de la seudonimización el uso de funciones criptográficas hash, las cuales transforman un dato en una cadena fija de caracteres denominada código hash, que no puede ser revertida para obtener el dato original. Sin embargo, si se dispone de un código hash y se conoce el universo de posibles valores de origen (por ejemplo, todos los números de DNI), resulta factible generar y contrastar listas de códigos hash correspondientes, lo que podría conducir a la reidentificación del titular del dato. En consecuencia, los datos personales tratados mediante funciones criptográficas hash también se encuentran sujetos la cumplimiento de la LPDP y el RLPDP.

Los algoritmos de encriptación bidireccional brindan seguridad, entre otros, al envío de correos electrónicos, transacciones bancarias, llamadas telefónicas; mientras que la función criptográfica hash (algoritmo de encriptación unidireccional) se emplea para el almacenamiento de contraseñas y otros datos sensibles que requieren de una verificación sin necesidad de conocer su contenido.

La seudonimización reduce el grado de vinculación entre un conjunto de datos con la identidad del titular; no obstante, se trata de una medida de seguridad complementaria y útil que puede emplear la entidad, incluso dentro de su misma área, pero no es una técnica de disociación ni anonimización por sí misma.

Ejemplo de aplicación de la función criptográfica Hash:

CUANDO UNA ENTIDAD PÚBLICA requiere gestionar las contraseñas de los correos institucionales de sus trabajadores durante el proceso de registro en un sistema web, no resulta adecuado almacenarlas en texto plano, ya que ello expondría dichas contraseñas en caso de filtración de la base de datos que las contiene. En su lugar, la entidad debe aplicar un algoritmo criptográfico de derivación de claves, como Argon2, que permite almacenar las contraseñas en forma de valores hash ilegibles bajo cualquier escenario. En este contexto, cuando el usuario del sistema inicia una nueva sesión, el sistema genera el hash de la clave ingresada por el usuario y lo compara con el valor previamente almacenado; si ambos coinciden, la autenticación se valida correctamente, sin que sea necesario conocer ni recuperar la contraseña original.

3

¿Cuándo y por qué disociar, anonimizar y seudonimizar datos personales?

3 ¿Cuándo y por qué disociar, anonimizar y seudonimizar datos personales?

¿Cuándo aplicar la disociación?

Cuando se busca reducir al máximo la reidentificación del titular del dato personal, pero se requiere mantener cierto nivel de información de dicho dato al momento de la entrega o publicación de la información, por lo que se aplicará en todos los escenarios de entrega y/o publicación de información estadística (que contiene datos personales) y en aquellos casos que se requiere conservar cierta información del dato publicado o entregado[6].

Casos de aplicación:

Al difundir, entregar o publicar:
- Reportes de diversa índole (de incidentes de seguridad, de encuestas o censos, etc).
- Bases de datos (con fines estadísticos, históricos o académicos).
- Registros clínicos o estadística clínica.

En todos estos escenarios, se necesita mantener cierto nivel de información del dato personal sin permitir su reconstrucción, por lo tanto, limitando la posibilidad de reidentificación del titular de los datos. En ciertos casos, es requisito mantener el dato intacto, mientras que en otros este debe quedar parcialmente oculto o modificarse por completo.

¿Cuándo aplicar la anonimización?

Cuando se quiera eliminar total y adecuadamente cualquier dato personal en un documento que pueda identificar, directa o indirectamente, a una o más personas.

Por tanto, se aplica sobre cualquier documento o archivo (expedientes, informes, resoluciones, cartas, requerimientos de información, solicitudes de acceso a la información pública, entre otros) a entregar y/o publicar que contenga datos personales respecto a los cuales resulte necesario impedir de manera razonable la reidentificación del titular o titulares del(los) dato(s).

6 Los ejemplos presentados en este documento tienen únicamente carácter ilustrativo y no constituyen una enumeración taxativa de la aplicación de la disociación. En ese sentido, los supuestos de aplicación de la disociación podrán comprender escenarios distintos y múltiples a los descritos, en la medida que se ajusten al propósito de la entrega y/o publicación de la información que contiene datos personales

¿Cuándo aplicar la seudonimización?

Para fines de la presente guía, se recomienda aplicar la seudonimización por cifrado bidireccional para la conservación, almacenamiento y tránsito de datos personales (bases de datos), siendo que, de ser implementado adecuadamente, permite el tratamiento seguro de datos personales.

Sin embargo, cuando se trata de datos personales que requieren una verificación de integridad sin conocer el dato, como es el caso de contraseñas de cuentas de usuario, es recomendable la aplicación de una función criptográfica HASH (cifrado unidireccional).

Casos de aplicación:

- Encriptación bidireccional: A modo general y a efectos prácticos, este mecanismo es aplicable a los datos almacenados en una base de datos, quedando a criterio de la entidad la selección de los datos a encriptar y del algoritmo empleado.
- Función criptográfica hash: Es aplicable para aquellos datos que, posteriormente, requerirán una validación de su integridad sin comprometer su contenido, como contraseñas.

¿Por qué disociar, anonimizar y seudonimizar?[7]

1. **Porque los datos personales** corresponden a sus titulares y no a las entidades públicas, por lo cual, sin perjuicio de las obligaciones establecidas por ley, se debe garantizar la protección y su adecuado tratamiento, de modo que no se afecte irrazonablemente la intimidad de las personas.

2. **Porque las entidades públicas,** en la actualidad, manejan grandes volúmenes de información que deben ser de fácil acceso y disposición para cualquier ciudadano; no obstante, existe también la obligación de proteger los datos personales y resguardarlos frente a cualquier exposición o tratamiento no autorizado.

3. **Porque la entidad pública** es la custodia de la información que crea y posee y de los datos personales que sus documentos (físicos o virtuales) contienen. Le corresponde, según el caso, un deber de confidencialidad en su tratamiento y de adopción de medidas de seguridad para evitar afectaciones y daños a los derechos del titular.

7 Si bien todos los puntos resultan aplicables a la disociación y anonimización, dado que su finalidad es la entrega y/o publicación de información que contiene datos personales, en el caso de la seudonimización estos también son pertinentes, salvo en lo referido a los puntos 04 y 05.

4 **Porque permite la entrega y publicación** de la información de manera adecuada y para los fines establecidos, salvaguardando la identificación del titular de los datos personales cuando deba hacerse, fomentando la confianza hacia las entidades públicas.

5 **Porque se evita la hipervisibilidad** de los datos personales de su titular; la cual, según el caso, puede generar situaciones vulneratorias de sus derechos a partir de la discriminación o estigmatización que pueda producir la asociación o indexación de dichos datos con informaciones que afecten su honor, reputación, intimidad o vida privada.

4

Criterios a considerar en los procedimientos de disociación, anonimización y seudonimización de datos personales

4 Criterios a considerar en los procedimientos de disociación, anonimización y seudonimización de datos personales

Para la aplicación adecuada de procedimientos de disociación, anonimización y seudonimización de información que contiene datos personales, es necesario, además de cumplir con la normativa de datos personales, adoptar ciertos criterios que permitan garantizar la eficacia de la(s) técnica(s) elegida(s); desde la fase inicial de revisión y selección de los datos personales presentes en la información, pasando por su tratamiento durante la aplicación de la técnica correspondiente, hasta llegar al resultado final. Dichos criterios se detallan a continuación:

4.1. Criterio de minimización de datos personales

La aplicación de técnicas de disociación o anonimización sobre datos personales debe realizarse únicamente sobre aquellos estrictamente necesarios para cumplir con la finalidad de publicación y/o entrega específica. Este criterio garantiza que los procedimientos empleados se apliquen únicamente sobre los datos indispensables para alcanzar el fin propuesto, preservando en todo momento la identidad de los titulares.

Es preciso señalar que este criterio guarda relación con el principio de finalidad en el tratamiento de datos personales (artículo 6 de la LPDP[8]), el cual establece que los datos personales deben ser recopilados para una finalidad determinada y explícita sin que puedan destinarse a una finalidad distinta de aquella que motivó su recopilación. De igual forma, se vincula con el principio de proporcionalidad (artículo 7 de la LPDP[9]), según el cual todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

No obstante, debe considerarse que ambos principios están referidos principalmente al tratamiento de datos personales en contextos donde los mismos son tratados de manera activa y se encuentran contenidos en un banco de datos personales. En contraste, el criterio de minimización de datos aquí

8 **Ley N.° 29733 – Ley de Protección de Datos Personales**
Artículo 6. Principio de finalidad
Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

9 **Ley N.° 29733 – Ley de Protección de Datos Personales**
Artículo 7. Principio de proporcionalidad
Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

analizado persigue un objetivo distinto: reducir al máximo el riesgo de reidentificación del titular de los datos personales, fortaleciendo de esta manera la protección de su privacidad.

Ejemplo 1:

Durante el procedimiento de disociación de datos personales efectuado sobre los resultados de una entrevista de trabajo, cuya finalidad es proporcionar información relevante sin permitir la reidentificación de los titulares, la entidad responsable aplica el criterio de minimización de datos para garantizar que, del conjunto total de datos recopilados, únicamente se apliquen las técnicas de disociación sobre aquellos datos estrictamente necesarios para cumplir con la finalidad declarada. De esta manera, se descartan que proporcionen información innecesaria del titular, tales como direcciones exactas, números de teléfono de contacto u otros que no resultan imprescindibles para el análisis.

Al aplicar este criterio, la entidad asegura que la información publicada conserve el valor para la atención de obligaciones propias de la función pública, sin perderla para registro histórico o administrativo. En consecuencia, el proceso de disociación solo disgrega datos personales no pertinentes para los fines que una entrevista de trabajo supone.

Ejemplo 2:

Una entidad dedicada a la materia laboral, con el fin de emitir un informe al público sobre la inserción laboral en estudiantes de los últimos años, solicita a una universidad pública la relación de todos los estudiantes del último ciclo de la carrera de Economía (décimo superior, quinto superior, tercio superior y regular) y el detalle de si en la actualidad se encuentran realizando prácticas preprofesionales.

Al respecto, la universidad, que posee el registro total de todos los estudiantes en una base de datos, aplica el principio de minimización y dependiendo del procedimiento de disociación o anonimización, selecciona los datos mínimos necesarios que serán sujetos a la aplicación de las técnicas elegidas.

En el presente caso, para efectos de elaborar dicho informe, los atributos denominados: "Alumno", "DNI", "Teléfono" y "Domicilio" no resultan relevantes y pueden ser suprimidos, para luego poder aplicar la técnica de disociación y anonimización respectiva; por lo cual, aplicando el principio de minimización de datos personales, la base de datos corresponde a la siguiente:

N.º	ALUMNO	EDAD	SEXO	DNI	TELÉFONO	DETALLE ALUMNO	DOMICILIO	REALIZA PRÁCTICAS PRE PROFESIONALES
1	Pepito Lucas Juárez Xzuw	16	M	401524538	942017	Tercio Superior	Jr. Las Azucenas 74AZ, San Sebastián	Sí
2	Lucas Pepito Diaz Fillow	19	M	701598751	845212	Regular	Av. La PC 88A2, San Rolan	No
3	Mateo Samuel Li Zaziga	25	M	067500526	884443	Regular	Condominio Los Rugrats 34e, Limita	No
4	Yeison Samuel Juárez Li	23	M	123485979	963144	Quinto Superior	Calle Orión 78Z, San Rebosio	Sí
5	Cima Express Audi Díaz	30	F	880102251	788123	Tercio Superior	Jr. Kion 10Q, Climent	No
6	Chelilla Parla Rebaza	17	F	123852064	440009	Regular	Los Trapecios 34eD, Lote 89, Otoño	No
7	Yisus Tonio Revoredo Grúa	17	M	993102475	331410	Quinto Superior	Av. Zunca 94W, Buena Vista	Sí
8	Carlos Alberto Pío Yucat	16	M	114889654	201933	Regular	Calle Don Boscoch 84W2, Los Claros	Sí
9	Anabell Histeria Sernia Huicho	23	F	089567412	874743	Regular	Calle, Las Maldivas 878C, Rio Bella	No
10	Ariel Simba Leña León	24	F	358946485	741785	Regular	Don Monti 34T, San Kilombo	No
11	Pepito Yoni Eloy Pacheco	25	M	987654321	100478	Décimo Superior	Jr. Tuestas 34V, Rio Bello	No
12	Luca Oli Todrich Guil	28	M	774035894	520314	Tercio Superior	Av. Amazonas 34-89, La Mariscala	Sí
13	Beatriz Ángela Moli Nava	29	F	874255845	894310	Regular	Calle Falsa 123, Spring, Illinno	No
14	Valentín Mejías Muente	22	M	486102598	846155	Quinto Superior	Calle la Paz 102Y, Mirafloristas	Sí
[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]
250	Manuel Alonso Chati Cruz	28	M	021589634	662143	Tercio Superior	Calle los Cedrosos 12R3, Colonia del Vals	Sí

Fuente: DGTAIPD del Minjusdh

N.º	EDAD	SEXO	DETALLE ALUMNO	REALIZA PRÁCTICAS PRE PROFESIONALES
1	16	M	Tercio Superior	Sí
2	19	M	Regular	No
3	25	M	Regular	No
4	23	M	Quinto Superior	Sí
5	30	F	Tercio Superior	No
6	17	F	Regular	No
7	17	M	Quinto Superior	Sí
8	16	M	Regular	Sí
9	23	F	Regular	No
10	24	F	Regular	No
11	25	M	Décimo Superior	No
12	28	M	Tercio Superior	Sí
13	29	F	Regular	No
14	22	M	Quinto Superior	Sí
[...]	[...]	[...]	[...]	[...]
250	28	M	Tercio Superior	Sí

Fuente: DGTAIPD del Minjusdh

Ejemplo 3:

Un ciudadano solicita a una entidad pública copia de un expediente administrativo sancionador que concluyó en el año 2022 con sanción al administrado, la cual ha sido cumplida. Al respecto, en la medida que el expediente contiene datos del administrado (persona natural) tales como sus nombres completos, dirección, DNI y número telefónico, y en la medida que se ha advertido que quien solicita la información es un tercero ajeno al procedimiento, la entidad pública remitirá el expediente sancionador aplicando el criterio de minimización de datos sobre los datos contenidos, para posteriormente aplicar las técnicas de disociación o anonimización correspondientes y necesarias para reducir el riesgo de reidentificación.

4.2. Privacidad desde el diseño y por defecto

La privacidad del diseño es un concepto transversal a los procedimientos de disociación, anonimización y seudonimización supone la aplicación de un enfoque que involucra la gestión del riesgo y la responsabilidad proactiva de la entidad pública, con la finalidad de asegurar la protección de los datos personales.

Para la disociación, la privacidad desde el diseño y por defecto implica que el tratamiento de los datos personales con fines de entrega y/o publicación sea planificado de manera que, desde su inicio, se definan cuáles serán los datos personales a seleccionar y las técnicas a emplear con la finalidad de minimizar el riesgo de reidentificación del titular. Sin embargo, es importante señalar que, por su naturaleza, la disociación implica que este proceso se redefina o actualice para cada caso particular, aunque se trate de la misma información de origen.

En cuanto a la anonimización, se trata de un caso particular, ya que es posible, para ciertos escenarios, prever de antemano qué datos personales se van a anonimizar. En ese sentido, la aplicación de este principio implica que el tratamiento de los datos personales con fines de entrega y/o publicación sea planificado de manera que, desde su inicio, se definan qué datos personales seleccionar y qué mecanismos de anonimización se aplicarán con la finalidad de minimizar el riesgo de reidentificación del titular.

En la seudonimización, ya que su finalidad no es la publicación o entrega de información, la privacidad desde el diseño y por defecto se traduce en que la entidad pública encargada del tratamiento de los datos personales debe definir a priori las medidas de seguridad para la protección de datos personales en lo concerniente a la arquitectura de los sistemas de información que los traten, al diseño de las bases de datos que los almacenarán, los algoritmos de cifrado que los encriptarán, la selección de aquellos datos personales que serán cifrados y las condiciones para su desencriptación (si es un cifrado bidireccional), entre otros.

Nota

Conforme a lo establecido en el numeral 3 del artículo 5 del DL 1412, Ley de Gobierno Digital[10], las entidades públicas deben cumplir con el **principio de privacidad desde el diseño,** durante el diseño y configuración de los servicios digitales que ofrecen a fin de garantizar la protección de los datos personales de los ciudadanos.

Ejemplos:

Disociación

El instituto nacional público cardiovascular recibe una solicitud de información por parte de una farmacéutica especializada, donde se requiere remitir información sintomatológica de pacientes con afecciones cardiacas particulares. Antes de iniciar con el proceso de disociación de la información a entregar, puesto que la entrega nominal no puede darse, la entidad pública debe asegurarse de definir, de acuerdo a la finalidad específica, la selección de los datos personales a disociar, las técnicas a aplicar, su modo de aplicación y los mecanismos de entrega de la información. Sin embargo, ya que la aplicación de las técnicas de disociación también depende del contexto tecnológico, es necesario que la privacidad desde el diseño se aplique para cada proceso de disociación, ello supondrá integrar medidas preventivas y de seguridad desde la etapa inicial de preparación de la información, prever riesgos de reidentificación, establecer protocolos claros de acceso y trazabilidad, así como documentar las decisiones adoptadas para garantizar transparencia, rendición de cuentas y cumplimiento normativo.

Anonimización

Una entidad pública implementará un portal de datos abiertos donde publicará resoluciones anonimizadas con fines informativos predeterminados. Ya que los tipos de datos personales a anonimizar y las técnicas a aplicar en un documento resolutivo pueden ser previstos, es posible para la entidad establecer un procedimiento de anonimización predeterminado, al que dichos documentos serán sujetos cuando corresponda.

Seudonimización: Encriptado bidireccional

Un instituto de enfermedades neoplásicas decide almacenar datos nominales de pacientes

10 **Decreto Legislativo N.º 1412 – Decreto Legislativo que aprueba la Ley de Gobierno Digital**
Artículo 5.- Principios rectores
Las disposiciones contenidas en la presente Ley, así como su aplicación se rigen por los siguientes principios rectores:
(...)
5.3 Privacidad desde el Diseño. - En el diseño y configuración de los servicios digitales se adoptan las medidas preventivas de tipo tecnológico, organizacional, humano y procedimental.

con cáncer en una base de datos a la cual le aplica la técnica de seudonimización por encriptado bidireccional; de modo, que la base de datos interna que almacene estos datos (texto ininteligible), sea accesible solo mediante sistemas que incorporen una llave de cifrado. Esto permite que, en caso de exposición o filtrado de la base de datos, estos no comprometan la identidad de los titulares de los datos personales.

Seudonimización: Función criptográfica hash

Una entidad supervisora cuenta con un sistema de información web destinado a ser empleado por sus contribuyentes, quienes deben registrarse y crear una cuenta de usuario en el sistema para acceder al mismo. La entidad, en lugar de almacenar la contraseña en texto plano, emplea un algoritmo de función criptográfica HASH para generar un código hash de la contraseña. Este código único e irreversible permite verificar que el dato personal ingresado en etapas posteriores sea el mismo que generó el código HASH almacenado por la entidad, sin necesidad de almacenar la contraseña en su forma original. No obstante, si se combinara el código hash con información adicional externa, podría facilitarse la reidentificación del titular, motivo por el cual su gestión debe hacerse bajo las medidas de seguridad establecidas en la LPDP y su Reglamento.

5

Pasos para realizar una correcta disociación y anonimización de datos personales

5 Pasos para realizar una correcta disociación y anonimización de datos personales

Los datos personales que han sido obtenidos por el responsable o encargado de su tratamiento deben tratarse conforme a la LPDP y su RLPDP, sin perjuicio de las responsabilidades de las entidades públicas en relación a lo dispuesto por la LTAIP y las normas sectoriales que correspondan.

A continuación, se detallan tres (3) pasos esenciales para llevar a cabo la disociación y anonimización de información que contiene datos personales:

1. Identificación y selección adecuada de datos personales

En esta fase, acorde al criterio de privacidad desde el diseño, la entidad responsable del procedimiento de disociación y anonimización debe identificar, de manera clara, los datos personales que serán sujetos a los procedimientos de disociación o anonimización, excluyendo, de acuerdo al criterio de minimización de datos, aquellos que no sean relevantes a la finalidad de la entrega y/o publicación de la información.

En el caso de la disociación, es posible que, partiendo de un mismo conjunto de datos se puedan aplicar procedimientos de disociación diferentes (cada uno distinto debido a la finalidad de la entrega y/o publicación), dando como resultado distintas versiones de la información disociada.

Así pues, se debe clasificar los datos personales atendiendo a las circunstancias de cada caso concreto.

Aplicaciones:

- **Para la disociación:** En el caso de aplicar la disociación, resulta necesario identificar previamente qué datos personales serán objeto de este procedimiento. Dichos datos deben transformarse de manera que solo conserven un valor informativo mínimo, suficiente para cumplir con la finalidad de la entrega y/o publicación de la información, pero sin permitir la identificación directa o indirecta del titular de los datos personales cuando no sea necesaria. Por ejemplo, al tratarse de la publicación de información estadística para investigación clínica, se deben únicamente seleccionar los datos personales (por ejemplo, datos del diagnóstico, tratamiento, etc., respecto a los datos generales del paciente) que aporten valor a la finalidad de la publicación (objeto del estudio).

- **Para la anonimización:** En los escenarios de anonimización, es necesario identificar y diferenciar los datos que deben permanecer en el documento (como los referidos a representantes legales, figuras públicas o determinadas fechas relevantes) de aquellos que deben ser completamente anonimizados, de modo que se elimine cualquier posibilidad de vincular la información con la identidad del titular de los datos personales. Por ejemplo, en la publicación de una resolución de un procedimiento administrativo sancionador, si se menciona al representante legal de una empresa, los datos de dicha persona tales como sus nombres completos, número de DNI o correo corporativo, no serán objeto de anonimización, en la medida en que actúa en representación de una persona jurídica y no a título personal.

Ejemplo:

Una entidad pública, a solicitud de un centro de investigación pública, debe entregar información sobre enfermedades infecciosas en la región de La libertad, con la finalidad de que se elabore un informe estadístico respecto a la incidencia de dichas enfermedades. La entidad pública tiene una base de datos con la siguiente información:

N.°	NOMBRES Y APELLIDOS	EDAD	DNI	TELÉFONO	DOMICILIO	HOSPITAL	ENFERMEDAD	FECHA DE DIAGNÓSTICO
1	Pepito Lucas Juárez Xzuw	16	401524538	942017	Jr. Las Azucenas 74AZ, San Sebastián	Hospital Público Central de Los Llanos	Nefrotoxiplasmosis Viral	11/01/2024
2	Lucas Pepito Diaz Fillow	19	701598751	845212	Av. La PC 88A2, San Rolan	Hospital Público Regional del Viento	Pneumocloritis Sónica	10/02/2024
3	Mateo Samuel Li Zaziga	25	067500526	884443	Condominio Los Rugrats 34e, Limita	Instituto Nacional de Salud Materno Infantil de Altomonte	Cerebrotaxia Filamentosa	26/03/2024
4	Mat Samuel Juárez Li	43	123485979	963144	Calle Orion 78Z, San Rebosio	Hospital Nacional de Cuidados Críticos "Ángel de la Guarda"	Hepatocloroma Viral	09/04/2024
5	Cima Express Audi Díaz	30	880102251	788123	Jr. Kion 10Q, Climent	Hospital Nacional de Enfermedades Tropicales "Selva Viva"	Enteromitosis Fluctuante	13/05/2024
6	Cellila Parla Rebaza	17	123852064	440009	Los Trapecios 34eD, Lote 89, Otoño	Instituto Nacional de Emergencias y Trauma "24 Horas"	Virosis Camaleónica de Tipo Z	22/05/2024
7	Yisus Tonio Revoredo Grúa	57	993102475	331410	Av. Zunca 94W, Buena Vista	Instituto Nacional de Salud del Trabajador "Manos Fuertes"	Nefrotoxiplasmosis Viral	03/06/2024
8	Carlos Alberto Pío Yucat	16	114889654	201933	Calle Don Boscoch 84W2, Los Claros	Hospital Público Central de Los Llanos	Hepatocloroma Viral	25/06/2024
9	Anabell Histeria Sernia Huicho	23	089567412	874743	Calle, Las Maldivas 878C, Rio Bella	Hospital General Regional "Valle de los Cedros"	Pilosarcina Migratoria	29/07/2024
10	Paulina Horacio Gregory Uma	33	358946485	741785	Don Monti 34T, San Kilombo	Instituto Nacional de Cuidados Intermedios y Largos Plazos "San Andrés"	Enteromitosis Fluctuante	30/08/2024
11	Sofía Mila Toche Guerra	25	987654321	100478	Jr. Tuestas 34V, Rio Bello	Centro Nacional de Salud Femenina "Clara Justicia"	Neuroleucoides Borboteantes	11/09/2024
12	Carlos Eduardo Jiménez Salazar	68	774035894	520314	Av. Amazonas 34-89, La Mariscala	Instituto Nacional de Salud Materno Infantil de Altomonte	Nefrotoxiplasmosis Viral	01/10/2024
13	Valeria Montserrat Aguirre León	29	874255845	894310	Calle Falsa 123, Spring, Illinno	Instituto Nacional de Emergencias y Trauma "24 Horas"	Pneumocloritis Sónica	18/10/2024
14	Luis Alberto González Mendoza	22	486102598	846155	Calle la Paz 102Y, Mirafloristas	Centro Nacional de Salud Femenina "Clara Justicia"	Rinofagia Vesiculosa	07/11/2024
15	María Fernanda Lopezalo García	28	021589634	662143	Calle los Cedrosos 12R3, Colonia del Vals	Centro Nacional de Salud Femenina "Clara Justicia"	Cerebrotaxia Filamentosa	04/12/2024
[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]
100	Clotilde Emma Simpson Park	70	998745026	023897	Calle, Las Palomas del Estanque 54R, Los Mellizos	Hospital Nacional de Cuidados Críticos "Ángel de la Guarda"	Nefrotoxiplasmosis Viral	15/12/2024

Fuente: DGTAIPD del Minjusdh

En ese sentido, la entidad pública debe identificar la información necesaria considerando, en este caso, la finalidad de la entrega. Así pues, procederá a clasificar los datos personales atendiendo a las circunstancias. En este caso, los datos personales de los pacientes advertidos son los siguientes: "Nombres y Apellidos", "Edad", "DNI", "Teléfono", "Domicilio", "Hospital", "Enfermedad" y "Fecha de diagnóstico".

Respecto a este paso, la entidad pública determina qué datos personales tiene la base de datos y procederá a identificar cuáles son necesarios. En el caso materia de ejemplo, la entidad pública identificó los datos personales del titular y advierte que no sería necesario identificar a los pacientes en tanto se requiere, en principio, información sobre las enfermedades infecciosas, por lo que, atendiendo al principio de minimización de datos personales, no considerará los atributos denominados "NOMBRES Y APELLIDOS ", "DNI", "TELÉFONO" y "DOMICILIO".

Supresión de columnas por criterio de minimización de datos personales

Información se mantiene

N.°	NOMBRES Y APELLIDOS	EDAD	DNI	TELÉFONO	DOMICILIO	HOSPITAL	ENFERMEDAD	FECHA DE DIAGNÓSTICO
1	Pepito Lucas Juárez Xzuw	16	401524538	942017	Jr. Las Azucenas 74AZ, San Sebastián	Hospital Público Central de Los Llanos	Nefrotoxiplasmosis Viral	11/01/2024
2	Lucas Pepito Diaz Fillow	19	701598751	845212	Av. La PC 88A2, San Rolan	Hospital Público Regional del Viento	Pneumocloritis Sónica	10/02/2024
3	Mateo Samuel Li Zaziga	25	067500526	884443	Condominio Los Rugrats 34e, Limita	Instituto Nacional de Salud Materno Infantil de Altomonte	Cerebrotaxia Filamentosa	26/03/2024
4	Mat Samuel Juárez Li	43	123485979	963144	Calle Orion 78Z, San Rebosio	Hospital Nacional de Cuidados Críticos "Ángel de la Guarda"	Hepatocloroma Viral	09/04/2024
5	Cima Express Audi Díaz	30	880102251	788123	Jr. Kion 10Q, Climent	Hospital Nacional de Enfermedades Tropicales "Selva Viva"	Enteromitosis Fluctuante	13/05/2024
6	Cellila Parla Rebaza	17	123852064	440009	Los Trapecios 34eD, Lote 89, Otoño	Instituto Nacional de Emergencias y Trauma "24 Horas"	Virosis Camaleónica de Tipo Z	22/05/2024
7	Yisus Tonio Revoredo Grúa	57	993102475	331410	Av. Zunca 94W, Buena Vista	Instituto Nacional de Salud del Trabajador "Manos Fuertes"	Nefrotoxiplasmosis Viral	03/06/2024
8	Carlos Alberto Pío Yucat	16	114889654	201933	Calle Do[illegible]	[illegible]ntral	Hepatocloroma Viral	25/06/2024
9	Anabell Histeria Sernia Huicho	23	089567412	874743	Calle, Las Maldivas 878C, Rio Bella	Hospital General Regional "Valle de los Cedros"	Pilosarcina Migratoria	29/07/2024
10	Paulina Horacio Gregory Uma	33	358946485	741785	Don Monti 34T, San Kilombo	Instituto Nacional de Cuidados Intermedios y Largos Plazos "San Andrés"	Enteromitosis Fluctuante	30/08/2024
11	Sofía Mila Toche Guerra	25	987654321	100478	Jr. Tuestas 34V, Rio Bello	Centro Nacional de Salud Femenina "Clara Justicia"	Neuroleucoides Borboteantes	11/09/2024
12	Carlos Eduardo Jiménez Salazar	68	774035894	520314	Av. Amazonas 34-89, La Mariscala	Instituto Nacional de Salud Materno Infantil de Altomonte	Nefrotoxiplasmosis Viral	01/10/2024

Información se mantiene

Fuente: DGTAIPD del Minjusdh

2. Evaluación de riesgos y aplicación de técnica(s) adecuadas

Una vez definidos los datos personales objeto de disociación o anonimización, se procede a una evaluación de riesgos orientada a identificar la probabilidad y el impacto de una eventual reidentificación de los titulares, considerando factores como la naturaleza de los datos personales seleccionados, la existencia de fuentes externas correlacionables, entre otros. En función de los resultados de dicha evaluación la entidad responsable determina la combinación de técnicas de disociación o, de corresponder, anonimización, más adecuadas para mitigar la identificación a un nivel aceptable.

Ahora bien, si durante la evaluación de riesgos la entidad pública advierte que los datos seleccionados podrían comprometer la confidencialidad del titular, resulta válido y recomendable reconsiderar la selección de datos, de manera que es posible ajustar el procedimiento de disociación o anonimización en esta fase, garantizando que la información publicada o entregada asegure razonablemente la

imposibilidad de reidentificar al titular de los datos personales. En este punto debe decidirse la intensidad de las técnicas aplicadas y verificar el resultado de la aplicación de las mismas.

Es importante mencionar que, a fin de reducir el riesgo de reidentificación en procedimientos de disociación, es altamente recomendable aplicar más de una técnica.

Se recomienda que la evaluación de impacto como los criterios utilizados para la selección de los datos personales queden debidamente documentados, ya que esta información constituye la evidencia fáctica de la aplicación de este paso, además de servir como insumo valioso en caso de una eventual reidentificación de los titulares de los datos personales disociados o anonimizados.

Aplicaciones:

- **Disociación:** En esta fase, la entidad pública, de acuerdo a la selección previa de datos personales, las técnicas a aplicar y a la finalidad de la publicación, realizará una evaluación respecto a la intensidad de las técnicas a aplicar, es decir, qué tanto disociar un dato personal mientras se conserva información del mismo y qué tan alta es la posibilidad de reidentificación a partir de los datos disociados.

- **Anonimización:** En esta etapa resulta fundamental verificar que los datos personales seleccionados y la técnica a aplicar sea realmente idónea para reducir el riesgo de reidentificación del titular de los datos personales. Si bien la anonimización busca eliminar (razonablemente) este riesgo, la entidad debe cerciorarse, mediante la evaluación de riesgos, que el nivel residual no sea alto, de esta forma, se garantiza que la publicación o entrega de la información cumpla con su finalidad sin comprometer la confidencialidad de los titulares.

Ejemplo:

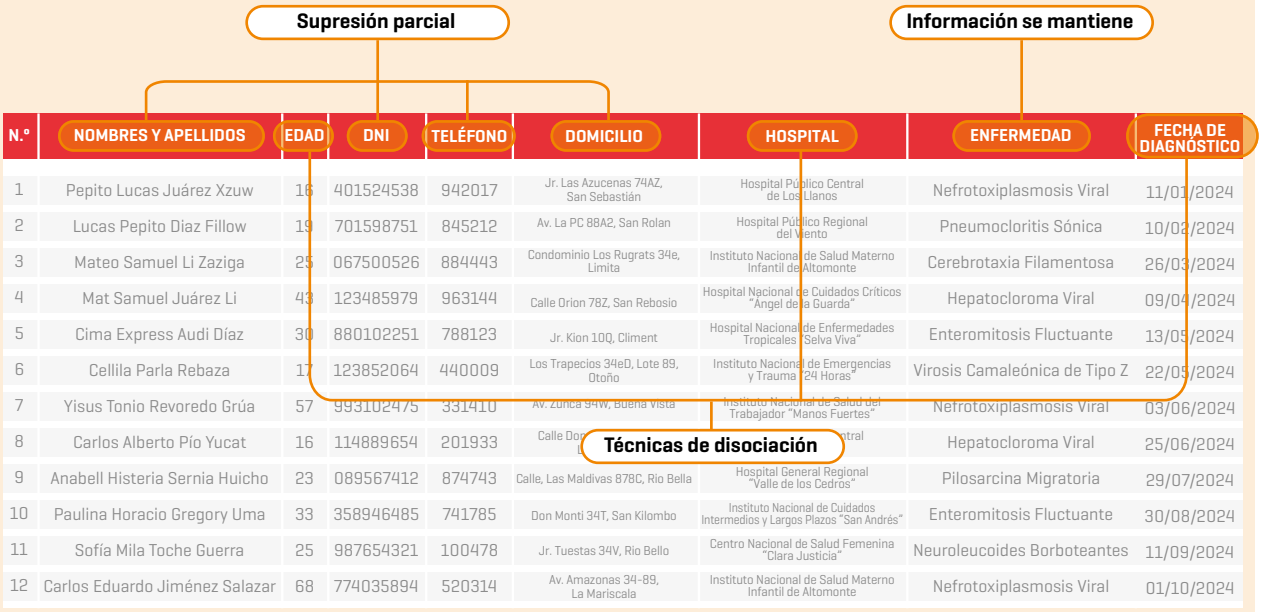
Atendiendo al ejemplo anterior, respecto a la información sobre enfermedades infecciosas a entregar, la entidad pública evaluará el riesgo de reidentificación de los titulares que presentan las enfermedades infecciosas. Por ejemplo, un riesgo podría ser que, si la enfermedad es poco frecuente en adquirirse solo en determinada zona, bastaría con identificar el nombre del hospital próximo o que se encuentre cerca de la región para poder obtener más datos que me lleven a la identificación del titular de datos personales.

En este caso, la entidad pública procederá a aplicar técnicas de disociación para los datos personales.

- Campos denominados "Nombres y Apellidos", "DNI", "Teléfono" y "Domicilio": En el paso anterior se aplicó la supresión de dichos campos por criterio de minimización de datos personales.

- Campos denominados "Edad", "Hospital", "Fecha de diagnóstico": Dicha información puede ser relevante y referencial con la finalidad que se busca, por lo cual se aplicarán diversas técnicas de disociación, de manera que se disminuya el riesgo de reidentificación del titular de los datos personales.

- Campo denominado "Enfermedad": Dicha información se mantiene dado que es necesaria para el análisis y la finalidad de la entrega de información



N.°	NOMBRES Y APELLIDOS	EDAD	DNI	TELÉFONO	DOMICILIO	HOSPITAL	ENFERMEDAD	FECHA DE DIAGNÓSTICO
1	Pepito Lucas Juárez Xzuw	16	401524538	942017	Jr. Las Azucenas 74AZ, San Sebastián	Hospital Público Central de Los Llanos	Nefrotoxiplasmosis Viral	11/01/2024
2	Lucas Pepito Díaz Fillow	19	701598751	845212	Av. La PC 88A2, San Rolan	Hospital Público Regional del Viento	Pneumocloritis Sónica	10/02/2024
3	Mateo Samuel Li Zaziga	25	067500526	884443	Condominio Los Rugrats 34e, Limita	Instituto Nacional de Salud Materno Infantil de Altomonte	Cerebrotaxia Filamentosa	26/03/2024
4	Mat Samuel Juárez Li	43	123485979	963144	Calle Orion 78Z, San Rebosio	Hospital Nacional de Cuidados Críticos "Ángel de la Guarda"	Hepatocloroma Viral	09/04/2024
5	Cima Express Audi Díaz	30	880102251	788123	Jr. Kion 10Q, Climent	Hospital Nacional de Enfermedades Tropicales "Selva Viva"	Enteromitosis Fluctuante	13/05/2024
6	Cellila Parla Rebaza	17	123852064	440009	Los Trapecios 34eD, Lote 89, Otoño	Instituto Nacional de Emergencias y Trauma "24 Horas"	Virosis Camaleónica de Tipo Z	22/05/2024
7	Yisus Tonio Revoredo Grúa	57	993102475	331410	Av. Zonca 94W, Buena Vista	Instituto Nacional de Salud del Trabajador "Manos Fuertes"	Nefrotoxiplasmosis Viral	03/06/2024
8	Carlos Alberto Pío Yucat	16	114889654	201933	Calle Do[illegible]	[illegible]ntral	Hepatocloroma Viral	25/06/2024
9	Anabell Histeria Sernia Huicho	23	089567412	874743	Calle, Las Maldivas 878C, Río Bella	Hospital General Regional "Valle de los Cedros"	Pilosarcina Migratoria	29/07/2024
10	Paulina Horacio Gregory Uma	33	358946485	741785	Don Monti 34T, San Kilombo	Instituto Nacional de Cuidados Intermedios y Largos Plazos "San Andrés"	Enteromitosis Fluctuante	30/08/2024
11	Sofía Mila Toche Guerra	25	987654321	100478	Jr. Tuestas 34V, Río Bello	Centro Nacional de Salud Femenina "Clara Justicia"	Neuroleucoides Borboteantes	11/09/2024
12	Carlos Eduardo Jiménez Salazar	68	774035894	520314	Av. Amazonas 34-89, La Mariscala	Instituto Nacional de Salud Materno Infantil de Altomonte	Nefrotoxiplasmosis Viral	01/10/2024

Fuente: DGTAIPD del Minjusdh

En ese sentido la entidad pública entregará la siguiente base de datos con la información solicitada, atendiendo a la finalidad de la investigación, siendo que en los campos "Edad", "Hospital" y "Fecha de diagnóstico" se utilizó la técnica de disociación de datos personales denominada generalización, mientras que respecto al campo "Enfermedad" no se realizó ningún cambio, conforme de muestra a continuación:

N.°	EDAD	HOSPITAL	ENFERMEDAD	FECHA DE DIAGNÓSTICO
1	15-25	Hospital Público (zona norte)	Nefrotoxiplasmosis Viral	Primer trimestre 2024
2	15-25	Hospital Público (zona sur)	Pneumocloritis Sónica	Primer trimestre 2024
3	15-25	Hospital Público (zona oeste)	Cerebrotaxia Filamentosa	Primer trimestre 2024
4	36-45	Hospital Público (zona este)	Hepatocloroma Viral	Segundo trimestre 2024
5	26-35	Hospital Público (zona norte)	Enteromitosis Fluctuante	Segundo trimestre 2024
6	15-25	Hospital Público (zona oeste)	Virosis Camaleónica de Tipo Z	Segundo trimestre 2024
7	56-65	Hospital Público (zona sur)	Nefrotoxiplasmosis Viral	Segundo trimestre 2024
8	15-25	Hospital Público (zona sur)	Hepatocloroma Viral	Segundo trimestre 2024
9	15-25	Hospital Público (zona oeste)	Pilosarcina Migratoria	Tercer trimestre 2024
10	26-35	Hospital Público (zona este)	Enteromitosis Fluctuante	Tercer trimestre 2024
11	15-25	Hospital Público (zona norte)	Neuroleucoides Borboteantes	Tercer trimestre 2024
12	66 a más	Hospital Público (zona norte)	Nefrotoxiplasmosis Viral	Cuarto trimestre 2024

Fuente: DGTAIPD del Minjusdh

3. Monitoreo del procedimiento de disociación o anonimización

El encargado o responsable del tratamiento de datos personales debe evaluar de manera periódica la eficacia de las técnicas aplicadas. Esto responde a que la filtración de bases de datos o la disponibilidad de nuevas herramientas tecnológicas permite incrementar el riesgo de reidentificación de los titulares, por lo que resulta necesario establecer mecanismos de revisión continua. Dicho monitoreo debe contemplar tanto la verificación de la idoneidad de las técnicas utilizadas como la detección de eventuales vulnerabilidades vinculadas a la identificación del titular, a fin de obtener información respecto a la mejora de futuros procesos de anonimización o disociación.

En consecuencia, el monitoreo continuo debe orientarse a los procedimientos futuros de disociación o anonimización, tomando como referencia la revisión de experiencias previas y complementándola con un análisis actualizado del contexto y de la realidad tecnológica. El propósito de este ejercicio es incorporar las lecciones aprendidas y, en la medida de lo posible, ajustar y perfeccionar la aplicación de dichas técnicas, de modo que se refuerce progresivamente la protección de los datos personales frente a riesgos emergentes de reidentificación del titular.

Ejemplo:

Atendiendo al ejemplo antes señalado y aplicando este último paso, si bien se entregó la información solicitada, el encargado o responsable del tratamiento de datos personales debe evaluar periódicamente la eficacia de la(s) técnica(s) aplicada(s) en la base de datos que se encuentran en su custodia; en tanto, como se ha indicado, la aparición de nuevas tecnologías podría generar un riesgo de reidentificación, por lo cual resulta necesario la actualización del procedimiento aplicado a través del control posterior, para prevenir este riesgo, así como establecer procedimientos de control posterior para verificar la eficacia de la disociación o anonimización.

Nota

Es preciso indicar que los pasos señalados no son relevantes para la aplicación de las técnicas de seudonimización, ya que el objetivo de estas últimas no atiende a la publicación y/o entrega de información que no permita reidentificar al titular, sino al tratamiento seguro de los datos personales.

¡RECUERDA!

- **Las entidades públicas, como titulares de bancos de datos o responsables del tratamiento de datos personales,** adoptan las medidas de seguridad necesarias para garantizar la seguridad de los datos personales que administran en razón del ejercicio de sus competencias.

- **Las entidades públicas definen los perfiles** de quienes participarán en la disociación y anonimización; es decir, los usuarios que poseen la información, los técnicos informáticos, entre otros, velando porque cuenten con la formación necesaria para aplicar correctamente la técnica que garantice la privacidad de la información personal.

- **Las entidades públicas son responsables** de aplicar las técnicas y procedimientos de disociación o anonimización cuando van a entregar y/o publicar información, a fin de garantizar la privacidad de la información de los ciudadanos. La inobservancia de ello, puede generar responsabilidad administrativa por incumplimiento de la LPDP y el RLPDP, sin perjuicio de la responsabilidad disciplinaria del personal a cargo.

- **Las personas que en razón de sus funciones operan** o tienen acceso a los datos personales, más aún, datos personales sensibles, deben guardar reserva de dicha información, de acuerdo a lo dispuesto en el artículo 17 de la LPDP.

- **Si bien la disociación y anonimización son procedimientos** por los cuales se busca la salvaguarda de los datos personales con el fin de minimizar el riesgo de reidentificación del titular de los mismos, dependerá mucho de cada situación, dado que, por su particularidad o por alguna disposición sectorial normativa, determinados datos pueden o no ser sujetos a esta técnica.

- **La entidad pública siempre tiene en su poder** el documento original, y las técnicas de disociación y anonimización de datos personales se aplican a la información que sea materia de entrega y/o publicación para terceros o para conocimiento público.

- **Es fundamental distinguir entre los datos** que permiten identificar a las personas y aquellos que se refieren a los hechos objeto del proceso o procedimiento al que estén vinculados o hagan referencia. En general, debe tratarse con el debido cuidado toda aquella información relacionada con los hechos, ya que ello resulta crucial para valorar adecuadamente todo documento que contenga información relevante que pueda reidentificar al titular de los datos personales. Cuando dicha información pueda permitir la identificación de los individuos involucrados, deberá prevalecer la disociación de los datos personales.

- **La aplicación de las técnicas de disociación y anonimización** no limita el cumplimiento de los derechos de los titulares de los datos personales, en especial el derecho de información, así como la aplicación de las medidas de seguridad que deben garantizarse para evitar los riesgos de reidentificación.

6

Técnicas recomendadas para la entrega y/o publicación de información que contiene datos personales

6 Técnicas recomendadas para la entrega y/o publicación de información que contiene datos personales

6.1. Técnicas de Disociación

Las técnicas de disociación, en su finalidad, se caracterizan por mantener cierto nivel de información respecto al conjunto de datos entregado y/o publicado, minimizando el riesgo la reidentificación de los titulares de los datos implicados, de modo que terceros no puedan vincular a los titulares de los datos a partir del conjunto de datos disociados.

Cuando la entidad pública requiere disociar un conjunto de datos con finalidades de publicación y/o entrega, es necesario que esta genere una copia de dicha información, a fin de poder aplicar las técnicas elegidas sin comprometer la integridad de la información original, teniendo en cuenta el contexto tecnológico actual y atendiendo al tipo de información, objeto que se busca, tipo de datos que se están tratando, número de titulares involucrados, riesgo de identificación, consecuencias para el responsable y el titular, entre otros.

En la mayoría de casos y, sobre todo, respecto a la información digital destinada a ser publicada en portales o a través de datos abiertos, se requiere la aplicación no solo de múltiples técnicas de disociación que se complementen para disminuir el riesgo de reidentificación, sino que es necesario definir con claridad la intensidad de la aplicación de las técnicas elegidas. Por ejemplo, la aplicación de ruido sobre un dato podría ser tan alta que ocasionaría la pérdida de utilidad del dato publicado, sin embargo, aplicar poco ruido podría facilitar la reidentificación del titular de los datos personales.

Dentro de las técnicas de disociación más utilizadas encontramos:

6.1.1 Adición de ruido

Definición

Consiste en reducir la exactitud los datos personales seleccionados, conservando su utilidad, de modo tal, que no se permita la reidentificación de los titulares de los datos implicados por parte de un tercero con acceso a la información disociada, incluso por la propia entidad.

Ejemplo:

La edad o estatura de una persona se define como un número entero, sin embargo, al aplicar la técnica de adición de ruido, se pueden modificar los valores con una exactitud de ± 10 (Ejemplo: La estatura de una persona es de 1,70 cm., por lo que el conjunto de datos, aplicando dicha técnica, será desde 1.60 cm a 1.70 cm).

Data original

PERSONA	EDAD
Persona 1	18
Persona 2	25
Persona 3	31
Persona 4	44
Persona 5	29

Con adición de ruido

PERSONA	EDAD
Persona 1	11-20
Persona 2	21-30
Persona 3	31-40
Persona 4	41-50
Persona 5	21-30

Data original

PERSONA	ESTATURA
Persona 1	1.53 cm
Persona 2	1.66 cm
Persona 3	1.75 cm
Persona 4	1.45 cm
Persona 5	1.81 cm

Con adición de ruido

PERSONA	ESTATURA
Persona 1	1.43 cm – 1.63 cm
Persona 2	1.56 cm – 1.76 cm
Persona 3	1.65 cm – 1.85 cm
Persona 4	1.35 cm – 1.55 cm
Persona 5	1.71 cm – 1.91 cm

¿Cuándo usarla?

- ✔ Su uso es recomendable para la entrega y/o publicación de información estadística o de difusión general, en tanto la pérdida de precisión del dato reduce el riesgo de reidentificación.
- ✔ De considerar que la precisión de algún dato personal es relevante, la técnica de adición de ruido se combina con otras técnicas, de modo que se reduzca el riesgo de reidentificación al titular del dato personal.
- ✔ Se aplica mayormente sobre datos estructurados en tanto el formato del documento permita su edición.

A tomar en cuenta

La aplicación de la técnica de la adición del ruido dependerá de la cantidad y el tipo de información que se requiera y de las otras técnicas aplicadas complementariamente, así como del impacto que podría tener en caso se revelen los atributos protegidos. Esta técnica abarca al redondeo de datos, desplazamiento de fechas, u otras técnicas que signifiquen la pérdida de precisión por alteración controlada de parámetros.

La aplicación excesiva de la adición de ruido puede hacer que el dato personal pierda su finalidad (volviéndose poco útil o engañoso), por lo que su uso debe ser proporcional a lo que se busca. Por tanto, la intensidad de cada técnica dependerá de cada caso en particular y la entidad debe evaluar bien qué tanto ruido aplica.

6.1.2. Enmascaramiento de caracteres

Definición

Técnica que consiste en la modificación de ciertos caracteres de un dato personal, de modo que quede parcialmente oculto. Ello se realiza usando símbolos (por ejemplo: "*", "x", "▬", etc.) para reemplazar caracteres específicos, a fin que se mantenga visible solo parte del dato personal.

La técnica se aplica solo a una parte de los caracteres del atributo, dejando visible la estructura o parte de la información necesaria para su identificación parcial, sin que ello permita revelar el valor completo del dato personal.

Ejemplo 1:

Un director general de una entidad pública requiere a la Oficina de Recursos Humanos los resultados de la última encuesta de clima laboral en la que participaron los trabajadores de su área. Esta Oficina, con el fin de no identificar a los trabajadores, decide disociar los nombres de usuarios de sus cuentas de correo electrónico institucional; por lo que opta por aplicar la técnica del enmascaramiento de caracteres antes de entregar la información.

Base de datos personales original

TRABAJADOR	CORREO INSTITUCIONAL	RESULTADO CLIMA LABORAL
Trabajador 1	aslopez@gobiernoregionaldatito.gob.pe	11 (Regular)
Trabajador 2	juquispe@gobiernoregionaldatito.gob.pe	18 (Satisfactorio)
Trabajador 3	dtchavez@gobiernoregionaldatito.gob.pe	05 (Bajo)
Trabajador 4	rprodriguez@gobiernoregionaldatito.gob.pe	15 (Bueno)
Trabajador 5	gymendoza@gobiernoregionaldatito.gob.pe	19 (Satisfactorio)

Base de datos personales con enmascaramiento de caracteres

TRABAJADOR	CORREO INSTITUCIONAL	RESULTADO CLIMA LABORAL
Trabajador 1	XXXX@gobiernoregionaldatito.gob.pe	11 (Regular)
Trabajador 2	XXXX@gobiernoregionaldatito.gob.pe	18 (Satisfactorio)
Trabajador 3	XXXX@gobiernoregionaldatito.gob.pe	05 (Bajo)
Trabajador 4	XXXX@gobiernoregionaldatito.gob.pe	15 (Bueno)
Trabajador 5	XXXX@gobiernoregionaldatito.gob.pe	19 (Satisfactorio)

Documento con información editable

Base de datos personales original

TRABAJADOR	CORREO INSTITUCIONAL	RESULTADO CLIMA LABORAL
Trabajador 1	aslopez@gobiernoregionaldatito.gob.pe	11 (Regular)
Trabajador 2	juquispe@gobiernoregionaldatito.gob.pe	18 (Satisfactorio)
Trabajador 3	dtchavez@gobiernoregionaldatito.gob.pe	05 (Bajo)
Trabajador 4	rprodriguez@gobiernoregionaldatito.gob.pe	15 (Bueno)
Trabajador 5	gymendoza@gobiernoregionaldatito.gob.pe	19 (Satisfactorio)

Base con datos personales aplicando enmascaramiento

TRABAJADOR	CORREO INSTITUCIONAL	RESULTADO CLIMA LABORAL
Trabajador 1	XXXX @gobiernoregionaldatito.gob.pe	11 (Regular)
Trabajador 2	XXXX@gobiernoregionaldatito.gob.pe	18 (Satisfactorio)
Trabajador 3	XXXX@gobiernoregionaldatito.gob.pe	05 (Bajo)
Trabajador 4	XXXX@gobiernoregionaldatito.gob.pe	15 (Bueno)
Trabajador 5	XXXX@gobiernoregionaldatito.gob.pe	19 (Satisfactorio)

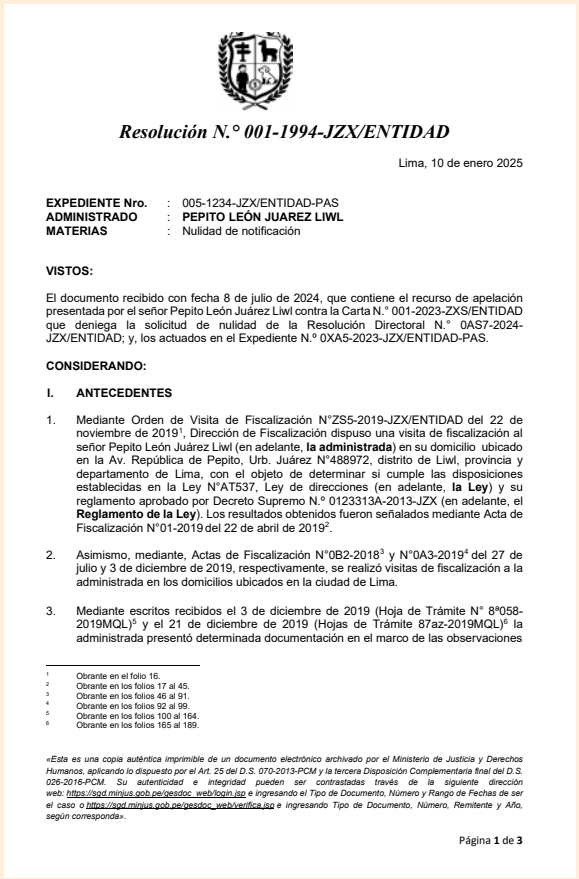
Fuente: DGTAIPD del Minjusdh

Ejemplo 2:

Una entidad pública requiere entregar la copia de un documento resolutivo, el cual fue generado a partir del escaneo del documento original, por lo que tanto el documento original como la copia sobre la que se aplicará el enmascaramiento serán imágenes. En esta situación restrictiva, la aplicación del enmascaramiento sobre el dato personal deberá realizarse sobre la imagen del dato y no directamente respecto al dato personal en texto. Para tal fin, la entidad empleará un software especializado, el cual permitirá reemplazar ciertos caracteres del dato personal mediante el pintado o dibujado del símbolo elegido para el enmascaramiento.

Nota

Es importante señalar que pueden presentarse escenarios en los que resulte inevitable entregar y/o publicar documentos en formatos no estructurados o semiestructurados (imágenes escaneadas, PDFs con diagramación compleja, etc), hecho que podría restringir la aplicación de técnicas de disociación (tales como enmascaramiento) y seudonimización, las cuales muestran su mayor eficacia cuando el tratamiento recae sobre datos estructurados.



Resolución N.° 001-1994-JZX/ENTIDAD

Lima, 10 de enero 2025

EXPEDIENTE Nro. : 005-1234-JZX/ENTIDAD-PAS
ADMINISTRADO : **PEPITO LEÓN JUAREZ LIWL**
MATERIAS : Nulidad de notificación

VISTOS:

El documento recibido con fecha 8 de julio de 2024, que contiene el recurso de apelación presentada por el señor Pepito León Juárez Liwl contra la Carta N.° 001-2023-ZXS/ENTIDAD que deniega la solicitud de nulidad de la Resolución Directoral N.° 0AS7-2024-JZX/ENTIDAD; y, los actuados en el Expediente N.° 0XA5-2023-JZX/ENTIDAD-PAS.

CONSIDERANDO:

I. ANTECEDENTES

1. Mediante Orden de Visita de Fiscalización N°ZS5-2019-JZX/ENTIDAD del 22 de noviembre de 2019[1], Dirección de Fiscalización dispuso una visita de fiscalización al señor Pepito León Juárez Liwl (en adelante, **la administrada**) en su domicilio ubicado en la Av. República de Pepito, Urb. Juárez N°488972, distrito de Liwl, provincia y departamento de Lima, con el objeto de determinar si cumple las disposiciones establecidas en la Ley N°AT537, Ley de direcciones (en adelante, **la Ley**) y su reglamento aprobado por Decreto Supremo N.° 0123313A-2013-JZX (en adelante, el **Reglamento de la Ley**). Los resultados obtenidos fueron señalados mediante Acta de Fiscalización N°01-2019 del 22 de abril de 2019[2].

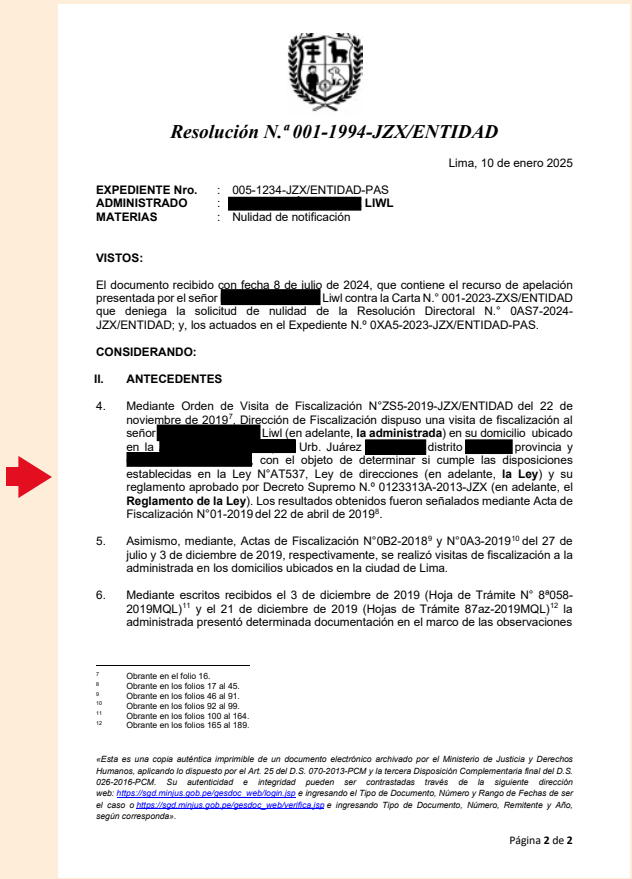
2. Asimismo, mediante, Actas de Fiscalización N°0B2-2018[3] y N°0A3-2019[4] del 27 de julio y 3 de diciembre de 2019, respectivamente, se realizó visitas de fiscalización a la administrada en los domicilios ubicados en la ciudad de Lima.

3. Mediante escritos recibidos el 3 de diciembre de 2019 (Hoja de Trámite N° 8°058-2019MQL)[5] y el 21 de diciembre de 2019 (Hojas de Trámite 87az-2019MQL)[6] la administrada presentó determinada documentación en el marco de las observaciones

1 Obrante en el folio 16.
2 Obrante en los folios 17 al 45.
3 Obrante en los folios 46 al 91.
4 Obrante en los folios 92 al 99.
5 Obrante en los folios 100 al 164.
6 Obrante en los folios 165 al 189.

«Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda».

Página **1** de **3**



Resolución N.ª 001-1994-JZX/ENTIDAD

Lima, 10 de enero 2025

EXPEDIENTE Nro. : 005-1234-JZX/ENTIDAD-PAS
ADMINISTRADO : [redacted] **LIWL**
MATERIAS : Nulidad de notificación

VISTOS:

El documento recibido con fecha 8 de julio de 2024, que contiene el recurso de apelación presentada por el señor [redacted] Liwl contra la Carta N.° 001-2023-ZXS/ENTIDAD que deniega la solicitud de nulidad de la Resolución Directoral N.° 0AS7-2024-JZX/ENTIDAD; y, los actuados en el Expediente N.° 0XA5-2023-JZX/ENTIDAD-PAS.

CONSIDERANDO:

II. ANTECEDENTES

4. Mediante Orden de Visita de Fiscalización N°ZS5-2019-JZX/ENTIDAD del 22 de noviembre de 2019[7], Dirección de Fiscalización dispuso una visita de fiscalización al señor [redacted] Liwl (en adelante, **la administrada**) en su domicilio ubicado en la [redacted] Urb. Juárez [redacted] distrito [redacted] provincia y [redacted] con el objeto de determinar si cumple las disposiciones establecidas en la Ley N°AT537, Ley de direcciones (en adelante, **la Ley**) y su reglamento aprobado por Decreto Supremo N.° 0123313A-2013-JZX (en adelante, el **Reglamento de la Ley**). Los resultados obtenidos fueron señalados mediante Acta de Fiscalización N°01-2019 del 22 de abril de 2019[8].

5. Asimismo, mediante, Actas de Fiscalización N°0B2-2018[9] y N°0A3-2019[10] del 27 de julio y 3 de diciembre de 2019, respectivamente, se realizó visitas de fiscalización a la administrada en los domicilios ubicados en la ciudad de Lima.

6. Mediante escritos recibidos el 3 de diciembre de 2019 (Hoja de Trámite N° 8°058-2019MQL)[11] y el 21 de diciembre de 2019 (Hojas de Trámite 87az-2019MQL)[12] la administrada presentó determinada documentación en el marco de las observaciones

7 Obrante en el folio 16.
8 Obrante en los folios 17 al 45.
9 Obrante en los folios 46 al 91.
10 Obrante en los folios 92 al 99.
11 Obrante en los folios 100 al 164.
12 Obrante en los folios 165 al 189.

«Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda».

Página **2** de **2**

Fuente: DGTAIPD del Minjusdh

¿Cuándo usarla?

- ✔ Para reemplazar un número fijo de caracteres en datos con estructura fija (como correos electrónicos), la aplicación dependerá del tipo de atributo que se tiene y con el que se quiera aplicar la técnica.
- ✔ En datos estructurados y semiestructurados no es recomendable si es que, al eliminar los datos seleccionados también se pierde la información esencial del dato. En su lugar, es mejor optar por otras técnicas más adecuadas de disociación o aplicar la anonimización respecto al documento editable.
- ✔ En formato físico se puede aplicar únicamente si no se cuenta con los medios digitales; así, se puede tomar una copia del original y aplicar un tachado físico o rayado parcial sobre el dato personal en el documento antes de su entrega. Para una mayor seguridad se recomienda realizar dicha técnica sobre la primera copia, siendo que la copia de la misma (segunda copia) sea la que finalmente se entregue al tercero.

6.1.3. Permutación

Definición

Técnica que implica reorganizar los datos personales en un conjunto de datos (bases de datos), de modo que estos se reasignen en un orden distinto respecto al titular de los datos.

Esta técnica busca que los atributos (características específicas) de un individuo aparezcan en otro registro, evitando que terceros puedan reidentificar al titular de los datos personales.

Se permite conservar las propiedades exactas del dato personal como la distribución y el rango de los valores, sin que se pueda asociar directamente al titular de los datos personales

Ejemplo:

Para temas de investigación en salud pública se requiere publicar el tipo de sangre de los pacientes mayores de edad hospitalizados en el Hospital Nacional Vida Saludable. En este caso, la entidad, para entregar la información y como parte del grupo de técnicas a aplicar efectuará la permutación:

Base de datos personales original

PACIENTE	EDAD	TIPO DE SANGRE
Paciente 1	44	AB-
Paciente 2	37	A+
Paciente 3	32	AB-
Paciente 4	18	O+
Paciente 5	21	O+
Paciente 6	50	O-
Paciente 7	32	B+

Base de datos personales aplicando permutación

Se permutan los atributos "Paciente", "Edad" y "Tipo de Sangre"

PACIENTE	EDAD	TIPO DE SANGRE
Paciente 3	18	O+
Paciente 4	25	AB-
Paciente 5	32	A+
Paciente 2	44	O-
Paciente 1	50	B+
Paciente 7	21	AB-
Paciente 6	37	O+

Fuente: DGTAIPD del Minjusdh

Del ejemplo mencionado, si bien se realizó la técnica de permutación, la información otorgada aún podría ser pasible de identificación al titular de datos personales, lo que reafirma la necesidad de combinar técnicas de disociación de forma complementaria.

¿Cuándo usarla?

- ✔ Para datos que principalmente contengan información estadística (ejemplo: datos para fines de investigación o para estudios de mercado) que requieran un alto índice de precisión. No se recomienda su uso aislado sino su combinación con otras técnicas.
- ✔ Sobre datos estructurados y semiestructurados, en la medida que los formatos que lo contengan puedan ser editables.

6.1.4. Generalización

Definición

Técnica que consiste en transformar valores específicos de datos personales por rangos o categorías más amplias que lo contengan. De esta manera, los datos generalizados se tornan menos específicos reduciendo la reidentificación del titular del dato personal.

Es muy importante ajustar previamente la aplicación de la técnica de acuerdo al objetivo del tratamiento de los datos personales, ello porque el generalizar demasiado podría ocasionar la pérdida de la utilidad de la información entregada y/o publicada, mientras que generalizar menos de lo requerido aumenta el riesgo de reidentificación del titular del dato personal.

Ejemplo:

Una entidad necesita publicar una lista que contenga el tipo de universidades a las que pertenecen determinados estudiantes, junto con información sobre su edad, vinculados a una zona geográfica específica. Para ello, opta por aplicar la técnica de generalización, dentro del conjunto de técnicas de disociación seleccionadas. En este caso, la entidad reemplaza la edad y el nombre de cada universidad por una categoría más amplia que, aunque proporciona información relevante, impide la identificación directa de los titulares.

Base de datos personales original

ESTUDIANTES	EDAD	UNIVERSIDADES
Estudiante 1	18	Universidad Privada del Este
Estudiante 2	25	Universidad Nacional de Letras
Estudiante 3	32	Universidad Privada el Sol
Estudiante 4	50	Universidad Privada Universal
Estudiante 5	44	Universidad Nacional del Ambiente

Base de datos personales con generalización

ESTUDIANTES	EDAD	UNIVERSIDADES
Estudiante 1	16-30	Universidad Privada
Estudiante 2	16-30	Universidad Nacional
Estudiante 3	20-45	Universidad Privada
Estudiante 4	25-55	Universidad Privada
Estudiante 5	20-45	Universidad Nacional

Fuente: DGTAIPD del Minjusdh

Como podemos observar, si bien se realizó la técnica de generalización, la información otorgada aún podría ser pasible de identificación al titular de datos personales; por lo que se deberán aplicar o combinar de forma complementaria otras técnicas de disociación.

¿Cuándo usarla?

- ✔ En conjuntos de datos que permitan su categorización (por ejemplo, datos con información de edades o referencias geográficas), por lo cual deberá de evaluarse con cuidado el nivel de especificidad de la información resultante.
- ✔ Cuando se desee entregar y/o publicar información estadística, sobre todo categórica. Al respecto, se deberá de evaluar con cuidado el nivel de especificidad de la información resultante.
- ✔ Recomendable para datos estructurados y semiestructurados, en la medida que los formatos que lo contengan puedan ser editables.

A tomar en cuenta:

Nota

- Resulta probable que la aplicación de una sola técnica de disociación no resulte ser eficiente en tanto sea pasible de identificación del titular de los datos personales, por lo cual, es fundamental comprender que las técnicas de disociación recomendadas deben complementarse con la finalidad de disminuir el riesgo de reidentificación.

- El criterio de aplicación para elegir las técnicas adecuadas depende de cada situación concreta en la cual es relevante determinar cuál es el objeto de la finalidad para la cual se entrega y/o publica la información y qué datos personales se necesitan proteger.
- El criterio de selección de los sistemas de información (software) para aplicar las técnicas de disociación recomendadas es responsabilidad de cada entidad pública, incluidas las consecuencias de su uso, así como es responsabilidad de las mismas mantener actualizados dichos sistemas.

6.1.5. Ejemplos de aplicación y combinación de técnicas de disociación

Ejemplo 1:

Con el objeto de fomentar políticas públicas de seguridad vial, una entidad estatal requiere publicar estadísticas (que incluyan, las edades de las víctimas, mes del accidente y detalle del vehículo) sobre los accidentes de tránsito ocurridos durante el 2023 en una provincia determinada del país, incluyendo las zonas (distritos) en donde sucedieron dichos accidentes. La entidad cuenta con una base de datos donde se almacena información relacionada a los accidentes de tránsito. El presente ejemplo detalla las fases prácticas de disociación, mostrando cómo los datos personales van variando según se aplican las técnicas seleccionadas.

1. Se tiene la siguiente información en la base de datos de la entidad pública responsable de implementar la política pública.

VÍCTIMA	DNI	EDAD	Dirección del accidente	Fecha del accidente	Hora del accidente	Detalles del vehículo
María Nieto	17185415	18	Calle A # 123, distrito Condemar	17/08/2023	19:35	Auto convertible
Martha Valverde	15574860	25	Avenida B # 654, distrito Waravía	15/09/2023	15:36	Motocicleta de carrera
José Romero	98954721	32	Jirón C # 456, distrito San Datito	21/01/2023	11:20	Camioneta
Pedro Páramo	65233074	44	Calle D #11, Distrito Los Robles	30/10/2023	04:22	Auto familiar

Fuente: DGTAIPD del Minjusdh

2. Como paso previo a la aplicación de las técnicas de disociación, la entidad estatal, atendiendo al criterio de minimización de datos personales, evaluará qué campos en el contenido de la base de datos son necesarios; por lo cual, en este proceso, procederá a eliminar los identificadores personales respecto a los atributos denominados "Víctima", "DNI" y "Hora del Accidente", tal como se aprecia a continuación:

Base de datos original

VÍCTIMA	DNI	EDAD	Dirección del accidente	Fecha del accidente	Hora del accidente	Detalles del vehículo
María Nieto	17185415	18	Calle A # 123, distrito Condemar	17/08/2023	19:35	Auto convertible
Martha Valverde	15574860	25	Avenida B # 654, distrito Waravía	15/09/2023	15:36	Motocicleta de carrera
José Romero	98954721	32	Jirón C # 456, distrito San Datito	21/01/2023	11:20	Camioneta
Pedro Páramo	65233074	44	Calle D #11, Distrito Los Robles	30/10/2023	04:22	Auto familiar

Fuente: DGTAIPD del Minjusdh

Aplicando el criterio de minimización de datos personales se realiza la supresión de los atributos "Víctima", "DNI" y "Hora del accidente", obteniendo el siguiente resultado:

EDAD	Dirección del accidente	Fecha del accidente	Detalles del vehículo
18	Calle A # 123, distrito Condemar	17/08/2023	Auto convertible
25	Avenida B # 654, distrito Waravía	15/09/2023	Motocicleta de carrera
32	Jirón C # 456, distrito San Datito	21/01/2023	Camioneta
44	Calle D #11, Distrito Los Robles	30/10/2023	Auto familiar

Fuente: DGTAIPD del Minjusdh

3. Una vez aplicado el criterio de minimización de datos personales, la entidad estatal procederá a aplicar las técnicas de disociación pertinentes para cumplir con la finalidad de lo solicitado, evitando la reidentificación de los titulares de datos personales. Por tanto, respecto al identificador denominado "Dirección del accidente", se aplicará la técnica de enmascaramiento específicamente a los números de las direcciones, lo cual permitirá la identificación del nombre de la calle y el distrito sin brindar más información respecto de la ubicación, conforme se muestra a continuación:

Base de datos enmascarada

EDAD	Dirección del accidente	Fecha del accidente	Detalles del vehículo
18	Calle A ****, distrito Condemar	17/08/2023	Auto convertible
25	Avenida B ****, distrito Waravía	15/09/2023	Motocicleta de carrera
32	Jirón C ****, distrito San Datito	21/01/2023	Camioneta
44	Calle D ****, distrito Los Robles	30/10/2023	Auto familiar

Fuente: DGTAIPD del Minjusdh

4. Posteriormente, se aplica la técnica de generalización para los demás identificadores personales (edad, fecha del accidente, detalles del vehículo) con la finalidad de mantener información útil para su análisis sin brindar detalles que permitan la reidentificación de las personas, de acuerdo al siguiente detalle:

Base de datos enmascarada

EDAD	Dirección del accidente	Fecha del accidente	Detalles del vehículo
18	Calle A ****, distrito Condemar	17/08/2023	Auto convertible
25	Avenida B ****, distrito Waravía	15/09/2023	Motocicleta de carrera
32	Jirón C ****, distrito San Datito	21/01/2023	Camioneta
44	Calle D ****, distrito Los Robles	30/10/2023	Auto familiar

Fuente: DGTAIPD del Minjusdh

Base de datos aplicando generalización

EDAD	Dirección del accidente	Fecha del accidente	Detalles del vehículo
18-24	Calle A ****, distrito Condemar	agosto 2023	Vehículo 4 ruedas
25-30	Avenida B ****, distrito Waravía	septiembre 2023	Vehículo 2 ruedas
30-35	Jirón C ****, distrito San Datito	enero 2023	Vehículo 4 ruedas
40-45	Calle D ****, distrito Los Robles	octubre 2023	Vehículo 4 ruedas

Fuente: DGTAIPD del Minjusdh

La edad se convirtió en un rango y respecto a la fecha del accidente y los detalles del vehículo dichos datos se categorizaron

5. Al final el conjunto de datos resultante se encuentra disociado al elegir adecuadamente las técnicas respectivas, brindando información valiosa sin permitir la identificación de los titulares de los datos personales, tal como se aprecia a continuación:

Base de datos original

VÍCTIMA	DNI	EDAD	Dirección del accidente	Fecha del accidente	Hora del accidente	Detalles del vehículo
María Nieto	17185415	18	Calle A # 123, distrito Condemar	17/08/2023	19:35	Auto convertible
Martha Valverde	15574860	25	Avenida B # 654, distrito Waravía	15/09/2023	15:36	Motocicleta de carrera
José Romero	98954721	32	Jirón C # 456, distrito San Datito	21/01/2023	11:20	Camioneta
Pedro Páramo	65233074	44	Calle D #11, Distrito Los Robles	30/10/2023	04:22	Auto familiar

Fuente: DGTAIPD del Minjusdh

Base de datos disociada

EDAD	Dirección del accidente	Fecha del accidente	Hora del accidente	Detalles del vehículo
18-24	Calle A ****	agosto 2023	12:00 – 20:00	Vehículo 4 ruedas
25-30	Avenida B ****	septiembre 2023	12:00 – 20:00	Vehículo 2 ruedas
30-35	Jirón C ****	enero 2023	00:00 – 12:00	Vehículo 4 ruedas
40-45	Calle D ****	octubre 2023	00:00 – 12:00	Vehículo 4 ruedas

Fuente: DGTAIPD del Minjusdh

Ejemplo 2:

Con el fin de poder dar a conocer la cantidad de productos entregados y las zonas beneficiadas en el rubro agrario, una entidad desea publicar un informe respecto al detalle de las cantidades de semillas de alcachofa certificadas distribuidas a los pequeños agricultores de toda la zona central del país; asimismo también informará de manera general si dichos agricultores también siembran otro tipo de alimentos.

1. Se tiene la siguiente información en la base de datos de la entidad pública:

N.°	NOMBRES Y APELLIDOS	EDAD	DNI	DOMICILIO	LOCALIDAD	CANTIDAD DE SEMILLAS DE ALCACHOFA [Kg]	SIEMBRA OTROS PRODUCTOS
1	Pepito Lucas Juárez Xzuw	56	401524538	Jr. Las Azucenas 74AZ, San Sebastián	Nueva Luz de la Montaña, Zona Sur	150	Papa y camote
2	Lucas Pepito Diaz Fillow	39	7015987517	Av. La PC 88A2, San Rolan	Santa Rosa del Valle, Zona Centro	120	Papa y camote
3	Mateo Samuel Li Zaziga	35	0675005263	Condominio Los Rugrats 34e, Limita	Colinas del Sol, Zona Norte	100	Yuca
4	Mat Samuel Juárez Li	43	123485979	Calle Orion 78Z, San Rebosio	Nueva Luz de la Montaña, Zona Sur	93	Choclo
5	Cima Express Audi Díaz	60	880102251	Jr. Kion 10Q, Climent	Nueva Luz de la Montaña, Zona Sur	42	Choclo
6	Cellila Parla Rebaza	57	123852064	Los Trapecios 34eD, Lote 89, Otoño	Colinas del Sol, Zona Norte	33	Papa y camote
7	Yisus Tonio Revoredo Grúa	39	993102475	Av. Zunca 94W, Buena Vista	Santa Rosa del Valle, Zona Centro	56	Yuca
8	Carlos Alberto Pío Yucat	47	114889654	Calle Don Boscoch 84W2, Los Claros	Nueva Luz de la Montaña, Zona Sur	180	Choclo
9	Anabel Histeria Serbia Huicho	46	089567412	Calle, Las Maldivas 878C, Rio Bella	Nueva Luz de la Montaña, Zona Sur	55	Yuca
10	Ariel Simba Leña León	54	358946485	Don Monti 34T, San Kilombo	Santa Rosa del Valle, Zona Centro	220	Papa y camote
[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]
320	María Fernanda Lopezalo García	47	845201365	Calle 8 Sur 15-60, Chapineirolis	Nueva Luz de la Montaña, Zona Sur	300	Papa y camote

Fuente: DGTAIPD del Minjusdh

2. En el marco de la finalidad de la publicación, como paso previo a la aplicación de las técnicas de disociación, la entidad estatal, atendiendo al criterio de minimización de datos personales, evaluará qué campos en el contenido de la base de datos son necesarios; por lo cual, en este proceso, procederá a eliminar los identificadores personales respecto a los atributos denominados "Nombres y Apellidos", "Edad", "DNI" y "Domicilio", tal como se aprecia a continuación:

Base de datos original

N.°	NOMBRES Y APELLIDOS	EDAD	DNI	DOMICILIO	LOCALIDAD	CANTIDAD DE SEMILLAS DE ALCACHOFA [Kg]	SIEMBRA OTROS PRODUCTOS
1	Pepito Lucas Juárez Xzuw	56	401524538	Jr. Las Azucenas 74AZ, San Sebastián	Nueva Luz de la Montaña, Zona Sur	150	Papa y camote
2	Lucas Pepito Diaz Fillow	39	7015987517	Av. La PC 88A2, San Rolan	Santa Rosa del Valle, Zona Centro	120	Papa y camote
3	Mateo Samuel Li Zaziga	35	0675005263	Condominio Los Rugrats 34e, Limita	Colinas del Sol, Zona Norte	100	Yuca
4	Mat Samuel Juárez Li	43	123485979	Calle Orion 78Z, San Rebosio	Nueva Luz de la Montaña, Zona Sur	93	Choclo
5	Cima Express Audi Díaz	60	880102251	Jr. Kion 10Q, Climent	Nueva Luz de la Montaña, Zona Sur	42	Choclo
6	Cellila Parla Rebaza	57	123852064	Los Trapecios 34eD, Lote 89, Otoño	Colinas del Sol, Zona Norte	33	Papa y camote
7	Yisus Tonio Revoredo Grúa	39	993102475	Av. Zunca 94W, Buena Vista	Santa Rosa del Valle, Zona Centro	56	Yuca
8	Carlos Alberto Pío Yucat	47	114889654	Calle Don Boscoch 84W2, Los Claros	Nueva Luz de la Montaña, Zona Sur	180	Choclo
9	Anabel Histeria Serbia Huicho	46	089567412	Calle, Las Maldivas 878C, Rio Bella	Nueva Luz de la Montaña, Zona Sur	55	Yuca
10	Ariel Simba Leña León	54	358946485	Don Monti 34T, San Kilombo	Santa Rosa del Valle, Zona Centro	220	Papa y camote
[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]
320	María Fernanda Lopezalo García	47	845201365	Calle 8 Sur 15-60, Chapineirolis	Nueva Luz de la Montaña, Zona Sur	300	Papa y camote

Fuente: DGTAIPD del Minjusdh

Aplicando el criterio de minimización de datos personales se realiza la supresión de los atributos "Nombres y Apellidos", "Edad", "DNI" y "Domicilio"

N.°	LOCALIDAD	CANTIDAD DE SEMILLAS DE ALCACHOFA (Kg)	SIEMBRA OTROS PRODUCTOS
1	Nueva Luz de la Montaña, Zona Sur	150	Papa y camote
2	Santa Rosa del Valle, Zona Centro	120	Papa y camote
3	Colinas del Sol, Zona Norte	100	Yuca
4	Nueva Luz de la Montaña, Zona Sur	93	Choclo
5	Nueva Luz de la Montaña, Zona Sur	42	Choclo
6	Colinas del Sol, Zona Norte	33	Papa y camote
7	Santa Rosa del Valle, Zona Centro	56	Yuca
8	Nueva Luz de la Montaña, Zona Sur	180	Choclo
9	Nueva Luz de la Montaña, Zona Sur	55	Yuca
10	Santa Rosa del Valle, Zona Centro	220	Papa y camote
[...]	[...]	[...]	[...]
320	Nueva Luz de la Montaña, Zona Sur	300	Papa y camote

Fuente: DGTAIPD del Minjusdh

3. Una vez aplicado el criterio de minimización de datos personales, la entidad estatal procederá a aplicar las técnicas de disociación pertinentes para cumplir con la finalidad de lo solicitado, evitando la reidentificación de los titulares de datos personales. Por tanto, respecto al identificador denominado "Siembra otros productos", se aplicará la técnica de permutación específicamente, en tanto dicha información se requiere a nivel general:

Base de datos aplicando de la técnica de permutación

N.°	LOCALIDAD	CANTIDAD DE SEMILLAS DE ALCACHOFA (Kg)	SIEMBRA OTROS PRODUCTOS
1	Nueva Luz de la Montaña, Zona Sur	150	Choclo
2	Santa Rosa del Valle, Zona Centro	120	Yuca
3	Colinas del Sol, Zona Norte	100	Papa y camote
4	Nueva Luz de la Montaña, Zona Sur	93	Yuca
5	Nueva Luz de la Montaña, Zona Sur	42	Papa y camote
6	Colinas del Sol, Zona Norte	33	Choclo
7	Santa Rosa del Valle, Zona Centro	56	Choclo
8	Nueva Luz de la Montaña, Zona Sur	180	Papa y camote
9	Nueva Luz de la Montaña, Zona Sur	55	Papa y camote
10	Santa Rosa del Valle, Zona Centro	220	Yuca
[...]	[...]	[...]	[...]
320	Nueva Luz de la Montaña, Zona Sur	300	Choclo

Fuente: DGTAIPD del Minjusdh

4. Visto que solo se quiere saber la localidad (Zona Norte, Centro y Sur), mas no el detalle del mismo, se procederá a aplicar la técnica de generalización para parte del indicador "Localidad", de acuerdo al siguiente detalle:

Base de datos con permutación

N.°	LOCALIDAD	CANTIDAD DE SEMILLAS DE ALCACHOFA (Kg)	SIEMBRA OTROS PRODUCTOS
1	Nueva Luz de la Montaña, Zona Sur	150	Choclo
2	Santa Rosa del Valle, Zona Centro	120	Yuca
3	Colinas del Sol, Zona Norte	100	Papa y camote
4	Nueva Luz de la Montaña, Zona Sur	93	Yuca
5	Nueva Luz de la Montaña, Zona Sur	42	Papa y camote
6	Colinas del Sol, Zona Norte	33	Choclo
7	Santa Rosa del Valle, Zona Centro	56	Choclo
8	Nueva Luz de la Montaña, Zona Sur	180	Papa y camote
9	Nueva Luz de la Montaña, Zona Sur	55	Papa y camote
10	Santa Rosa del Valle, Zona Centro	220	Yuca
[...]	[...]	[...]	[...]
320	Nueva Luz de la Montaña, Zona Sur	300	Choclo

Fuente: DGTAIPD del Minjusdh

Base de datos aplicando generalización

N.°	LOCALIDAD	CANTIDAD DE SEMILLAS DE ALCACHOFA (Kg)	SIEMBRA OTROS PRODUCTOS
1	Zona Sur	150	Yuca
2	Zona Centro	120	Choclo
3	Zona Norte	100	Papaya y camote
4	Zona Sur	93	Papa y camote
5	Zona Sur	42	Choclo
6	Zona Norte	33	Yuca
7	Zona Centro	56	Papa y camote
8	Zona Sur	180	Choclo
9	Zona Sur	55	Papa y camote
10	Zona Centro	220	Choclo
[...]	[...]	[...]	[...]
320	Zona Sur	300	Yuca

Fuente: DGTAIPD del Minjusdh

5. Al final el conjunto de datos resultante se encuentra disociado al elegir adecuadamente las técnicas respectivas, brindando información valiosa sin permitir la identificación de los titulares de los datos personales, tal como se aprecia a continuación:

Base de datos original

N.°	NOMBRES Y APELLIDOS	EDAD	DNI	DOMICILIO	LOCALIDAD	CANTIDAD DE SEMILLAS DE ALCACHOFA (Kg)	SIEMBRA OTROS PRODUCTOS
1	Pepito Lucas Juárez Xzuw	56	401524538	Jr. Las Azucenas 74AZ, San Sebastián	Nueva Luz de la Montaña, Zona Sur	150	Papa y camote
2	Lucas Pepito Diaz Fillow	39	7015987517	Av. La PC 88A2, San Rolan	Santa Rosa del Valle, Zona Centro	120	Papa y camote
3	Mateo Samuel Li Zaziga	35	0675005263	Condominio Los Rugrats 34e, Limita	Colinas del Sol, Zona Norte	100	Yuca
4	Mat Samuel Juárez Li	43	123485979	Calle Orion 78Z, San Rebosio	Nueva Luz de la Montaña, Zona Sur	93	Choclo
5	Cima Express Audi Díaz	60	880102251	Jr. Kion 10Q, Climent	Nueva Luz de la Montaña, Zona Sur	42	Choclo
6	Cellila Parla Rebaza	57	123852064	Los Trapecios 34eD, Lote 89, Otoño	Colinas del Sol, Zona Norte	33	Papa y camote
7	Yisus Tonio Revoredo Grúa	39	993102475	Av. Zunca 94W, Buena Vista	Santa Rosa del Valle, Zona Centro	56	Yuca
8	Carlos Alberto Pío Yucat	47	114889654	Calle Don Boscoch 84W2, Los Claros	Nueva Luz de la Montaña, Zona Sur	180	Choclo
9	Anabel Histeria Serbia Huicho	46	089567412	Calle, Las Maldivas 878C, Rio Bella	Nueva Luz de la Montaña, Zona Sur	55	Yuca
10	Ariel Simba Leña León	54	358946485	Don Monti 34T, San Kilombo	Santa Rosa del Valle, Zona Centro	220	Papa y camote
[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]
320	María Fernanda Lopezalo García	47	845201365	Calle 8 Sur 15-60, Chapineirolis	Nueva Luz de la Montaña, Zona Sur	300	Papa y camote

Fuente: DGTAIPD del Minjusdh

Base de datos disociada

N.°	LOCALIDAD	CANTIDAD DE SEMILLAS DE ALCACHOFA (Kg)	SIEMBRA OTROS PRODUCTOS
1	Zona Sur	150	Yuca
2	Zona Centro	120	Choclo
3	Zona Norte	100	Papa y camote
4	Zona Sur	93	Papa y camote
5	Zona Sur	42	Choclo
6	Zona Norte	33	Yuca
7	Zona Centro	56	Papa y camote
8	Zona Sur	180	Choclo
9	Zona Sur	55	Papa y camote
10	Zona Centro	220	Choclo
[...]	[...]	[...]	[...]
320	Zona Sur	300	Yuca

Fuente: DGTAIPD del Minjusdh

6.2. Técnicas de Anonimización

Las técnicas de anonimización aplicables a un documento que contenga datos personales dependen tanto de la naturaleza del documento como del medio en el que este será entregado. En ese sentido, la entidad responsable debe seleccionar la metodología adecuada considerando la finalidad de la entrega, el soporte del documento y las medidas necesarias para asegurar la imposibilidad de reidentificación.

Por ejemplo, si se requiere aplicar anonimización sobre un documento resolutivo almacenado en formato de imagen dentro de un archivo .PDF, y cuya entrega debe realizarse en copia digital, será indispensable el uso de un sistema de información o software especializado que permita modificar o eliminar los fragmentos de la imagen que contienen datos personales. De esta manera se asegura que, aun empleando medios electrónicos de ampliación, edición o recuperación de información, la lectura de dichos datos resulte técnicamente imposible.

Por el contrario, si la entrega se efectúa en soporte físico y el documento original también se encuentra en dicho formato, corresponde que la entidad genere una copia intermedia del documento sobre la cual se aplicará la técnica de anonimización seleccionada (por ejemplo, tachado indeleble, borrado físico). Ello permite garantizar que el documento final entregado al solicitante no contenga información que comprometa la identidad de los titulares.

Debe tenerse presente que las técnicas de anonimización se caracterizan por impedir la identificación de los titulares de los datos personales y por imposibilitar que un tercero, mediante procedimientos razonables, logre restaurar la información original o inferir cómo fue modificada. En consecuencia, a diferencia de la disociación, la anonimización constituye un procedimiento irreversible, lo cual la convierte en una herramienta idónea cuando la finalidad de la publicación o entrega del documento no requiere preservar la trazabilidad individual de los datos.

Si bien la anonimización constituye un procedimiento irreversible, este carácter no es absoluto, pues la evolución tecnológica y la disponibilidad de nuevas fuentes de información pueden generar, con el tiempo, riesgos de reidentificación. Por ello, la entidad debe reevaluar periódicamente los procesos aplicados, considerando el contexto tecnológico y legal vigente. Asimismo, aunque el objetivo es alcanzar un nivel de anonimización total, en la práctica puede subsistir un riesgo residual de reidentificación —significativamente menor al de la disociación— que debe ser reconocido y gestionado adecuadamente.

A continuación, se detalla la siguiente técnica propia a utilizarse:

6.2.1. Aplicación de anonimización en documentos: Tachado

Definición

La técnica de tachado consiste en la eliminación u ocultamiento permanente de datos personales dentro de un documento, mediante su marcación, cobertura o supresión total, de modo que no puedan ser leídos ni recuperados por terceros. Su finalidad es asegurar que la información entregada o publicada por la entidad reduzca al mínimo el riesgo de reidentificación de los titulares de los datos.

En el ámbito **físico**, esta técnica se aplica sobre documentos impresos, utilizando medios indelebles (por ejemplo, tinta oscura, franjas opacas o bloqueos mecánicos) que imposibiliten la lectura de la información original, aun empleando métodos de ampliación o iluminación.

En el ámbito **digital**, el tachado se realiza sobre archivos electrónicos —como documentos en formato PDF o Word— empleando software especializado que no solo cubra visualmente los datos, sino que también elimine el contenido subyacente en el código del archivo. Esto garantiza que los datos no puedan ser recuperados mediante copiado, extracción de texto, inspección de metadatos o herramientas de edición digital.

En ambos casos, el tachado debe aplicarse de manera íntegra, verificable y con criterios de consistencia, asegurando que la versión final del documento sea apta para su difusión sin comprometer la confidencialidad de los titulares de los datos personales.

EJEMPLO DE LA TÉCNICA DE TACHADO (FÍSICO Y DIGITAL)

Una persona natural presenta una solicitud ante una entidad pública para obtener copia de una Resolución Directoral que se encuentra archivada en soporte físico en la Oficina de Recursos Humanos. Dicho documento contiene datos personales sensibles vinculados a un procedimiento disciplinario, tales como el nombre completo, el número de DNI y el domicilio del trabajador involucrado.

Con el fin de garantizar la entrega de la información solicitada sin vulnerar los derechos de protección de datos personales, la entidad aplica la técnica de tachado.

Para fines de ejemplificación práctica, se describen los escenarios posibles según el formato de entrega:

Entrega en formato físico

Escenario A: Tachado digital previo y entrega impresa
La entidad realiza primero una copia digital del documento original y aplica técnicas de tachado mediante un software de edición especializado. Posteriormente, imprime la versión digital anonimizada y la entrega al solicitante en soporte físico. En este caso, el documento entregado no permite la reconstrucción de los datos personales eliminados, aun empleando técnicas de ampliación o copiado.

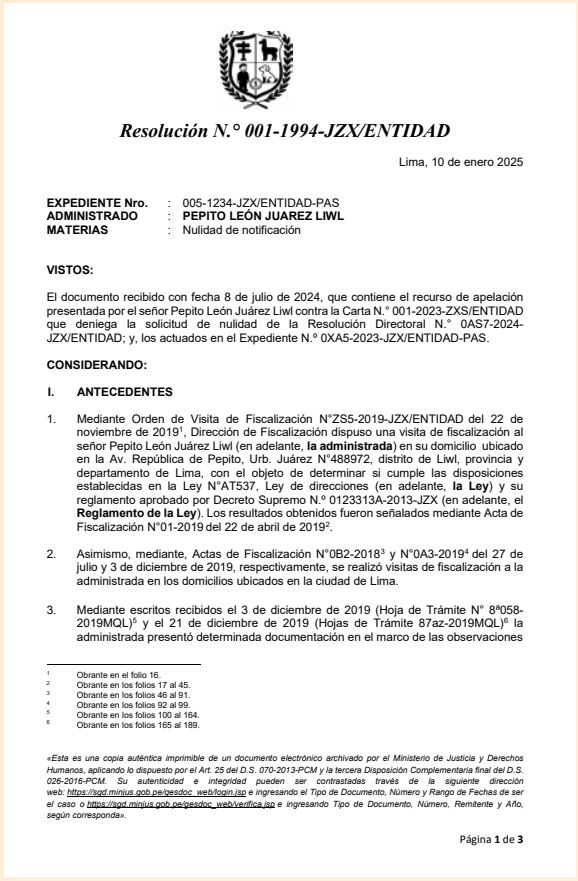
Escenario B: Tachado físico
La entidad obtiene una copia física del documento original y procede a aplicar el tachado manual de los datos personales mediante tinta negra indeleble. Luego, a fin de reforzar la irreversibilidad, genera una segunda copia de este documento ya tachado, la cual es finalmente entregada al solicitante. De este modo, se evita que la versión entregada muestre rastros visibles del dato original.

Entrega en formato digital

Tachado digital y entrega electrónica
La entidad digitaliza el documento original y aplica el tachado mediante un software con funciones de redacción, que no solo oculta visualmente los datos personales, sino que elimina también el contenido subyacente en el archivo (texto, metadatos o capas de imagen). Finalmente, entrega al solicitante una copia digital en formato PDF anonimizado, garantizando que la información cubierta no pueda ser visualizada ni recuperada por ningún medio electrónico.

Ejemplo (tachado digital y entrega electrónica):
Una persona natural solicita a una entidad pública copia de una resolución que se encuentra en su custodia y que cuenta con datos personales que podrían vulnerar la intimidad de su titular si estos se difunden, por lo que la entidad deberá de aplicar la mencionada técnica.

Siguiendo las instrucciones del ejemplo anterior, se tiene finalmente lo siguiente:



Resolución N.° 001-1994-JZX/ENTIDAD

Lima, 10 de enero 2025

EXPEDIENTE Nro. : 005-1234-JZX/ENTIDAD-PAS
ADMINISTRADO : **PEPITO LEÓN JUAREZ LIWL**
MATERIAS : Nulidad de notificación

VISTOS:

El documento recibido con fecha 8 de julio de 2024, que contiene el recurso de apelación presentada por el señor Pepito León Juárez Liwl contra la Carta N.° 001-2023-ZXS/ENTIDAD que deniega la solicitud de nulidad de la Resolución Directoral N.° 0AS7-2024-JZX/ENTIDAD; y, los actuados en el Expediente N.° 0XA5-2023-JZX/ENTIDAD-PAS.

CONSIDERANDO:

I. ANTECEDENTES

1. Mediante Orden de Visita de Fiscalización N°ZS5-2019-JZX/ENTIDAD del 22 de noviembre de 2019[1], Dirección de Fiscalización dispuso una visita de fiscalización al señor Pepito León Juárez Liwl (en adelante, **la administrada**) en su domicilio ubicado en la Av. República de Pepito, Urb. Juárez N°488972, distrito de Liwl, provincia y departamento de Lima, con el objeto de determinar si cumple las disposiciones establecidas en la Ley N°AT537, Ley de direcciones (en adelante, **la Ley**) y su reglamento aprobado por Decreto Supremo N.° 0123313A-2013-JZX (en adelante, el **Reglamento de la Ley**). Los resultados obtenidos fueron señalados mediante Acta de Fiscalización N°01-2019 del 22 de abril de 2019[2].

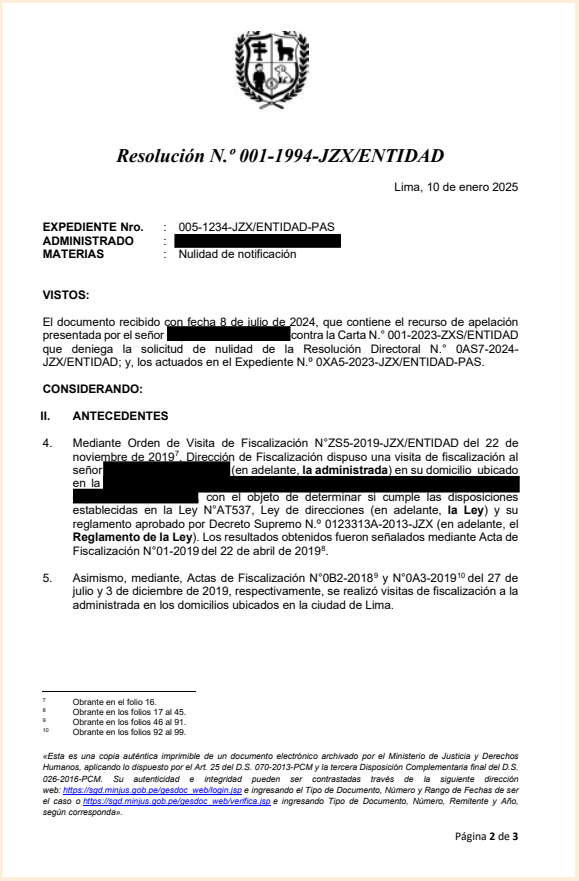
2. Asimismo, mediante, Actas de Fiscalización N°0B2-2018[3] y N°0A3-2019[4] del 27 de julio y 3 de diciembre de 2019, respectivamente, se realizó visitas de fiscalización a la administrada en los domicilios ubicados en la ciudad de Lima.

3. Mediante escritos recibidos el 3 de diciembre de 2019 (Hoja de Trámite N° 8ª058-2019MQL)[5] y el 21 de diciembre de 2019 (Hojas de Trámite 87az-2019MQL)[6] la administrada presentó determinada documentación en el marco de las observaciones

1 Obrante en el folio 16.
2 Obrante en los folios 17 al 45.
3 Obrante en los folios 46 al 91.
4 Obrante en los folios 92 al 99.
5 Obrante en los folios 100 al 164.
6 Obrante en los folios 165 al 189.

«Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda».

Página **1** de **3**



Resolución N.° 001-1994-JZX/ENTIDAD

Lima, 10 de enero 2025

EXPEDIENTE Nro. : 005-1234-JZX/ENTIDAD-PAS
ADMINISTRADO : [redacted]
MATERIAS : Nulidad de notificación

VISTOS:

El documento recibido con fecha 8 de julio de 2024, que contiene el recurso de apelación presentada por el señor [redacted] contra la Carta N.° 001-2023-ZXS/ENTIDAD que deniega la solicitud de nulidad de la Resolución Directoral N.° 0AS7-2024-JZX/ENTIDAD; y, los actuados en el Expediente N.° 0XA5-2023-JZX/ENTIDAD-PAS.

CONSIDERANDO:

II. ANTECEDENTES

4. Mediante Orden de Visita de Fiscalización N°ZS5-2019-JZX/ENTIDAD del 22 de noviembre de 2019[7], Dirección de Fiscalización dispuso una visita de fiscalización al señor [redacted] (en adelante, **la administrada**) en su domicilio ubicado en la [redacted] con el objeto de determinar si cumple las disposiciones establecidas en la Ley N°AT537, Ley de direcciones (en adelante, **la Ley**) y su reglamento aprobado por Decreto Supremo N.° 0123313A-2013-JZX (en adelante, el **Reglamento de la Ley**). Los resultados obtenidos fueron señalados mediante Acta de Fiscalización N°01-2019 del 22 de abril de 2019[8].

5. Asimismo, mediante, Actas de Fiscalización N°0B2-2018[9] y N°0A3-2019[10] del 27 de julio y 3 de diciembre de 2019, respectivamente, se realizó visitas de fiscalización a la administrada en los domicilios ubicados en la ciudad de Lima.

7 Obrante en el folio 16.
8 Obrante en los folios 17 al 45.
9 Obrante en los folios 46 al 91.
10 Obrante en los folios 92 al 99.

«Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda».

Página **2** de **3**

Fuente: DGTAIPD del Minjusdh

Ejemplo 2:

Una investigadora que realiza una investigación sobre violencia escolar de los últimos cinco (5) años le pide a la UGEL Datito que, por la vía digital, le remita copia de la base de datos que da cuenta de estos episodios en los colegios de su jurisdicción. La UGEL, consciente de lo innecesario de consignar datos nominales para el propósito del estudio, decide aplicar la técnica de anonimización por tachado en su base de datos.

Respecto a un documento estructurado, se puede realizar este procedimiento empleando por ejemplo un programa (software) que contenga la funcionalidad de "censura", "planchado" o afines sobre los datos personales implicados para la técnica. Dicha funcionalidad debe aplicarse únicamente sobre la versión del documento que será entregado o publicado, de lo contrario, es posible borrar la información de manera irrecuperable.

N.°	NOMBRES Y APELLIDOS	DNI	EDAD	DOMICILIO	AÑO
1	Pepito Lucas Juárez Xzuw	401524538	17	Scipión Llona N.° 350A, Miraflores, Lima	2024
2	Lucas Pepito Diaz Fillow	7015987517	15	Scipión Llona N.° 350B, Miraflores, Lima	2024
3	Mateo Samuel Li Zaziga	0675005263	11	Scipión Llona N.° 350C, Miraflores, Lima	2023
4	Carlos Alberto Pío Yucat	993102475	13	Scipión Llona N.° 350D, Miraflores, Lima	2023
5	Anabel Histeria Serbia Huicho	114889654	10	Scipión Llona N.° 350E, Miraflores, Lima	2022
6	[...]	[...]	[...]	[...]	[...]
83	Ariel Simba Leña León	358946485	8	Scipión Llona N.° 350ZA, Miraflores, Lima	2020

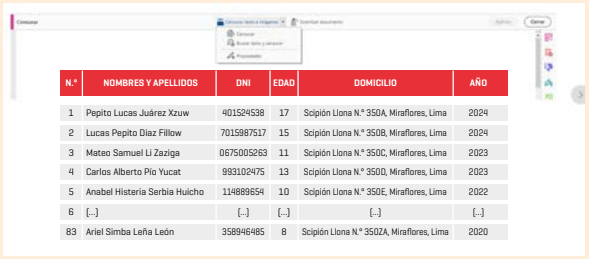


Tabla (contenida en el informe) suprimida

N.°	NOMBRES Y APELLIDOS	DNI	EDAD	DOMICILIO	AÑO
1	[redacted]	[redacted]	[redacted]	[redacted]	2024
2	[redacted]	[redacted]	[redacted]	[redacted]	2024
3	[redacted]	[redacted]	[redacted]	[redacted]	2023
4	[redacted]	[redacted]	[redacted]	[redacted]	2023
5	[redacted]	[redacted]	[redacted]	[redacted]	2022
6	[...]	[...]	[...]	[...]	[...]
7	[redacted]	[redacted]	[redacted]	[redacted]	2020

Fuente: DGTAIPD del Minjusdh

¿Cuándo usarla?

- ✔ En datos no estructurados y semiestructurados se puede aplicar el tachado total en documentos (por ejemplo, PDF de un documento por grandes volúmenes de textos o información) a través de un software que permita la edición del mismo.
- ✔ En formato físico, si no se cuenta con los medios digitales, se puede tomar una copia del original y aplicar un tachado físico o rayado total sobre el dato personal en el documento antes de su entrega. Para una mayor seguridad se recomienda realizar dicha técnica sobre la primera copia, siendo que la copia de la misma (segunda copia) sea la que finalmente se entregue al tercero.
- ✔ Su uso no es recomendable para datos estructurados, ya que el eliminar toda la información supone que el contenido esencial pierde su valor informativo. En su lugar, es mejor optar por técnicas más adecuadas como la disociación y seudonimización, especialmente respecto al documento editable.

EJEMPLOS DE APLICACIÓN DE ANONIMIZACIÓN EN DOCUMENTOS

Debido a las particularidades que implica la publicación de documentos por parte de las entidades públicas —ya sea en portales de datos abiertos o en el marco de la atención de solicitudes de acceso a la información pública— es posible para la entidad, en ciertos casos, anticipar y definir los datos personales que deberán ser anonimizados en documentos cuya estructura y contenido son conocidos de antemano.

En este sentido, la entidad puede establecer estándares de anonimización específicos según el tipo de documento a publicar y/o entregar, es decir, si dicho documento contiene o no información de naturaleza pública, sea el documento originado en la propia entidad o que provenga de fuente distinta (de persona natural ajena a la entidad, por ejemplo). Tratándose de información a entregar, la anonimización puede aplicarse para tachar datos personales de documentos que, en su conjunto, puedan generar el riesgo de identificar a una persona.

Así, por ejemplo, para aplicar el procedimiento de anonimización de un expediente en custodia de una entidad pública, corresponderá que, quien asume la obligación de entregar copia del mismo a quien lo solicita, tenga que tachar todos los datos personales de cada documento que puedan significar un riesgo para la reidentificación del titular de los mismos. Eso podrá significar que se tache datos como los siguientes[11]:

- Recibos por honorarios: para anonimizar datos personales como nombres completos, domicilio, monto a recibir, entre otros.
- Números de tarjetas de créditos o información crediticia: para anonimizar datos personales como nombres completos, historial de consultas de crédito, tipos de créditos utilizados, cantidad de deuda, entre otros.
- Contratos por prestación de servicios: para anonimizar datos personales como nombres completos, pago por entregable, domicilio, entre otros.
- Resoluciones: para anonimizar datos personales como nombres completos, DNI, teléfono, correo electrónico, profesión, entre otros.
- Informes: para anonimizar datos personales como nombres completos, DNI, teléfono, correo electrónico, entre otros.
- Declaración Anual del Impuesto a la Renta: para anonimizar datos personales como nombres DNI, teléfono, correo electrónico, montos relacionados con ingresos, entre otros.

11 Es preciso señalar que, los ejemplos incluidos en la presente guía tienen carácter ilustrativo y, entre otros, no resultan necesariamente aplicables a los casos que involucren a personas que ejercen cargos públicos, presten servicios al Estado o cumplen funciones públicas. En tales supuestos, la información que se difunda se rige por las disposiciones de la LTAIP, así como por su reglamento y demás normas complementarias o sectoriales, respectivamente.

- Fichas RENIEC: para anonimizar datos personales como nombres completos, número de DNI, fecha de nacimiento, firma, estatura, domicilio, imagen de la persona, entre otros.
- Boletas de pago: para anonimizar datos personales como nombres completos, ingresos, concepto de deducciones, entre otros.
- Historial médico, diagnósticos médicos, entre otros datos de salud: para anonimizar datos personales como nombres completos, número de DNI, teléfono, correo electrónico, fecha de nacimiento, peso, talla, diagnóstico, enfermedades preexistentes, operaciones, entre otros.
- Números telefónicos de personas naturales: para anonimizar datos personales como nombres completos, número telefónicos.
- Información que contenga el Documento Nacional de Identidad o la fotografía de dicho documento: para anonimizar datos personales como nombres completos, número de DNI, imagen de la persona, firma, entre otros.
- Antecedentes penales, judiciales, policiales: para anonimizar datos personales como nombres completos, número de DNI, delitos, infracciones, entre otros.

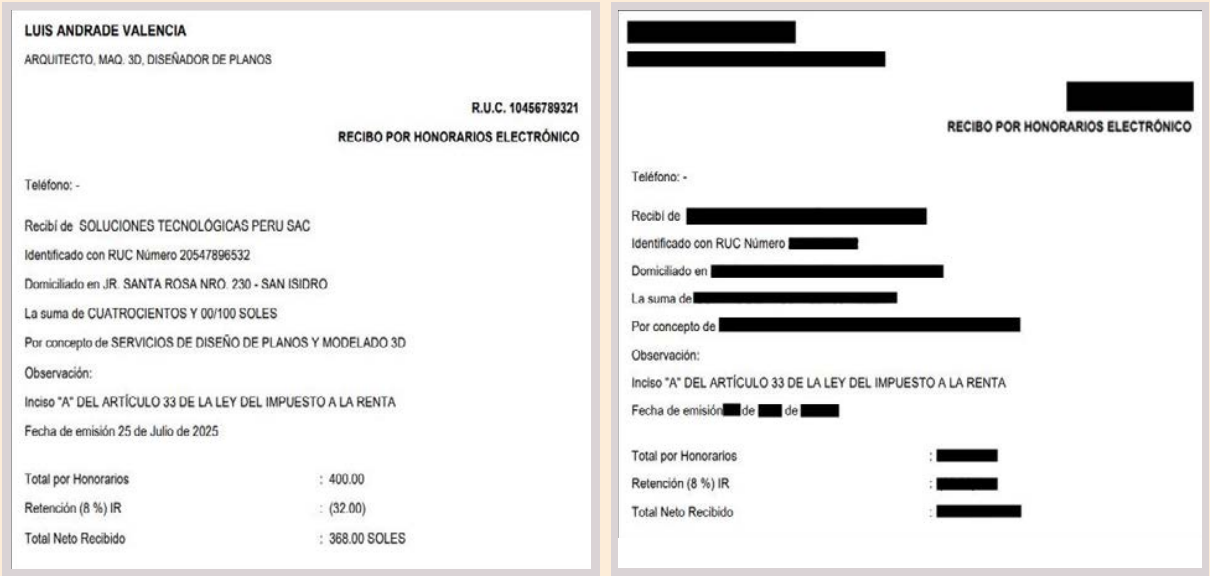
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO
FICHA DE DATOS PERSONALES

DNI:	12345678
Apellidos y Nombres:	JUAREZ BRAVO, PEPITO
Fecha de Nacimiento:	01/01/1990
Sexo:	Masculino
Nacionalidad:	Peruana
Estado Civil:	Soltero
Grado de Instrucción:	Universitaria Completa
Domicilio:	Av. Los Ficticios N.° 456, Urb. Imaginaria, San Borja, Lima

REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO
FICHA DE DATOS PERSONALES

DNI: [redacted]
Apellidos y Nombres: [redacted]
Fecha de Nacimiento: [redacted]
Sexo: [redacted]
Nacionalidad: [redacted]
Estado Civil: [redacted]
Grado de Instrucción: [redacted]
Domicilio: [redacted]

Fuente: DGTAIPD del Minjusdh



LUIS ANDRADE VALENCIA
ARQUITECTO, MAQ. 3D, DISEÑADOR DE PLANOS

R.U.C. 10456789321
RECIBO POR HONORARIOS ELECTRÓNICO

Teléfono: -

Recibí de SOLUCIONES TECNOLÓGICAS PERU SAC
Identificado con RUC Número 20547896532
Domiciliado en JR. SANTA ROSA NRO. 230 - SAN ISIDRO
La suma de CUATROCIENTOS Y 00/100 SOLES
Por concepto de SERVICIOS DE DISEÑO DE PLANOS Y MODELADO 3D
Observación:
Inciso "A" DEL ARTÍCULO 33 DE LA LEY DEL IMPUESTO A LA RENTA
Fecha de emisión 25 de Julio de 2025

Total por Honorarios	: 400.00
Retención (8 %) IR	: (32.00)
Total Neto Recibido	: 368.00 SOLES

[redacted]

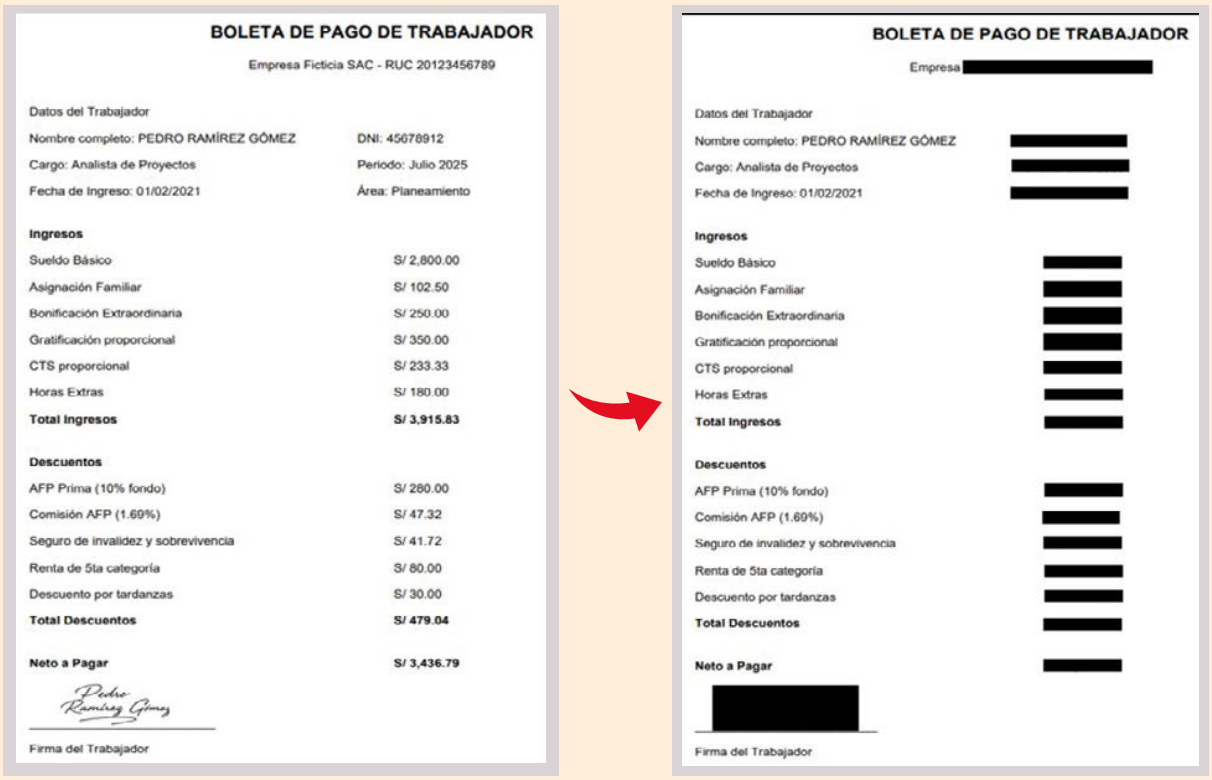
RECIBO POR HONORARIOS ELECTRÓNICO

Teléfono: -

Recibí de [redacted]
Identificado con RUC Número [redacted]
Domiciliado en [redacted]
La suma de [redacted]
Por concepto de [redacted]
Observación:
Inciso "A" DEL ARTÍCULO 33 DE LA LEY DEL IMPUESTO A LA RENTA
Fecha de emisión [redacted] de [redacted] de [redacted]

Total por Honorarios	: [redacted]
Retención (8 %) IR	: [redacted]
Total Neto Recibido	: [redacted]

Fuente: DGTAIPD del Minjusdh



BOLETA DE PAGO DE TRABAJADOR

Empresa Ficticia SAC - RUC 20123456789

Datos del Trabajador

Nombre completo: PEDRO RAMÍREZ GÓMEZ — DNI: 45678912

Cargo: Analista de Proyectos — Periodo: Julio 2025

Fecha de Ingreso: 01/02/2021 — Área: Planeamiento

Ingresos	
Sueldo Básico	S/ 2,800.00
Asignación Familiar	S/ 102.50
Bonificación Extraordinaria	S/ 250.00
Gratificación proporcional	S/ 350.00
CTS proporcional	S/ 233.33
Horas Extras	S/ 180.00
Total Ingresos	**S/ 3,915.83**

Descuentos	
AFP Prima (10% fondo)	S/ 280.00
Comisión AFP (1.69%)	S/ 47.32
Seguro de invalidez y sobrevivencia	S/ 41.72
Renta de 5ta categoría	S/ 80.00
Descuento por tardanzas	S/ 30.00
Total Descuentos	**S/ 479.04**

Neto a Pagar — **S/ 3,436.79**

Firma del Trabajador

BOLETA DE PAGO DE TRABAJADOR

Empresa [redacted]

Datos del Trabajador

Nombre completo: PEDRO RAMÍREZ GÓMEZ [redacted]

Cargo: Analista de Proyectos [redacted]

Fecha de Ingreso: 01/02/2021 [redacted]

Ingresos	
Sueldo Básico	[redacted]
Asignación Familiar	[redacted]
Bonificación Extraordinaria	[redacted]
Gratificación proporcional	[redacted]
CTS proporcional	[redacted]
Horas Extras	[redacted]
Total Ingresos	[redacted]

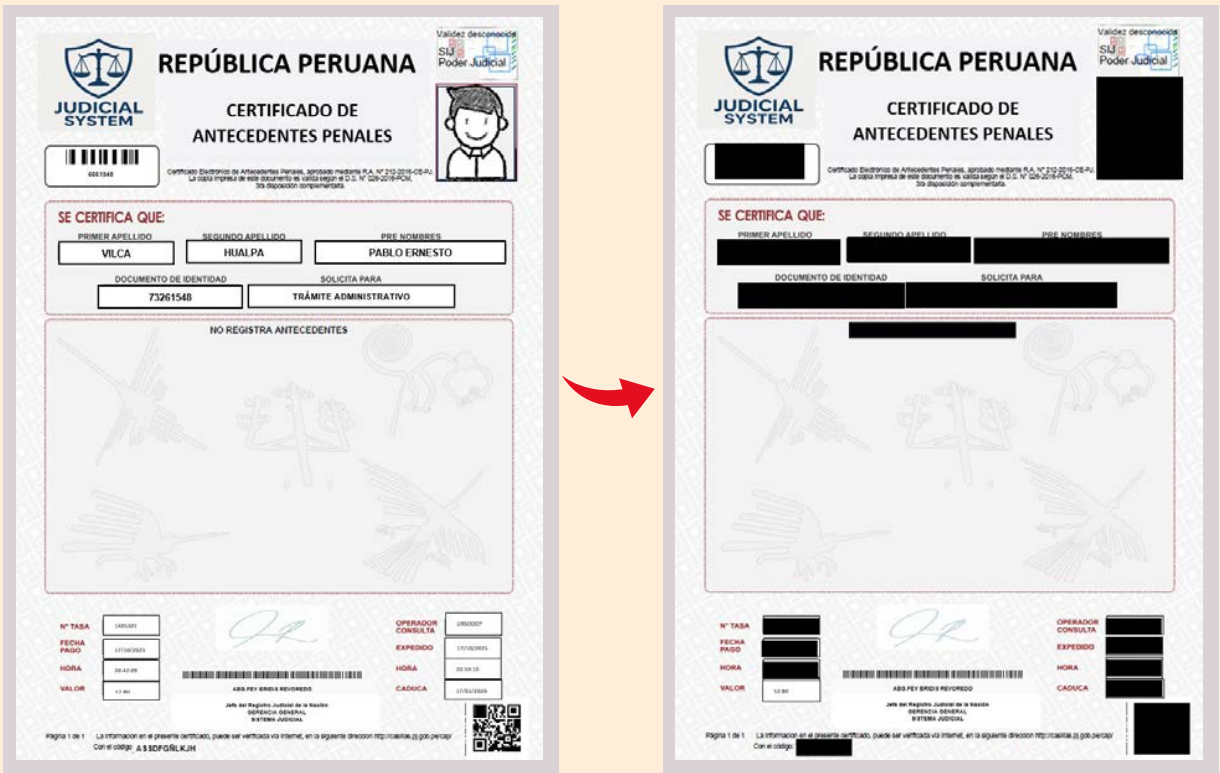
Descuentos	
AFP Prima (10% fondo)	[redacted]
Comisión AFP (1.69%)	[redacted]
Seguro de invalidez y sobrevivencia	[redacted]
Renta de 5ta categoría	[redacted]
Descuento por tardanzas	[redacted]
Total Descuentos	[redacted]

Neto a Pagar [redacted]

[redacted]

Firma del Trabajador

Fuente: DGTAIPD del Minjusdh



JUDICIAL SYSTEM

REPÚBLICA PERUANA

Validez desconocida — SIJ Poder Judicial

CERTIFICADO DE ANTECEDENTES PENALES

Certificado Electrónico de Antecedentes Penales, aprobado mediante R.A. N° 212-2016-CE-PJ. La copia impresa de este documento es valida según el D.S. N° 026-2016-PCM, 3ra disposición complementaria.

SE CERTIFICA QUE:

PRIMER APELLIDO	SEGUNDO APELLIDO	PRE NOMBRES
VILCA	HUALPA	PABLO ERNESTO

DOCUMENTO DE IDENTIDAD	SOLICITA PARA
73261548	TRÁMITE ADMINISTRATIVO

NO REGISTRA ANTECEDENTES

N° TASA — FECHA PAGO — HORA — VALOR — OPERADOR CONSULTA — EXPEDIDO — HORA — CADUCA

ABG.FEY BRIGIS REYOREGO

Jefa del Registro Judicial de la Nación
GERENCIA GENERAL
SISTEMA JUDICIAL

Página 1 de 1 — La información en el presente certificado, puede ser verificada vía internet, en la siguiente dirección http://scertss.pj.gob.pe/cap
Con el código: A$3DFGÑLKJH

JUDICIAL SYSTEM

REPÚBLICA PERUANA

Validez desconocida — SIJ Poder Judicial

CERTIFICADO DE ANTECEDENTES PENALES

Certificado Electrónico de Antecedentes Penales, aprobado mediante R.A. N° 212-2016-CE-PJ. La copia impresa de este documento es valida según el D.S. N° 026-2016-PCM, 3ra disposición complementaria.

SE CERTIFICA QUE:

PRIMER APELLIDO	SEGUNDO APELLIDO	PRE NOMBRES
[redacted]	[redacted]	[redacted]

DOCUMENTO DE IDENTIDAD	SOLICITA PARA
[redacted]	[redacted]

[redacted]

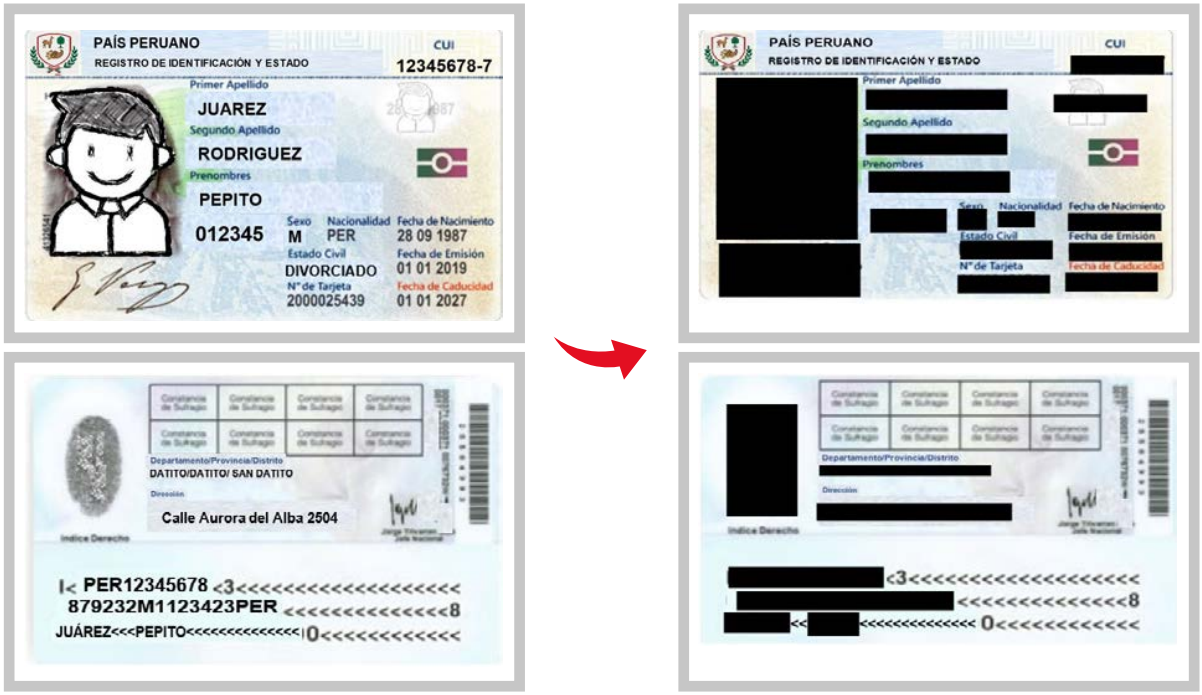
N° TASA — FECHA PAGO — HORA — VALOR — OPERADOR CONSULTA — EXPEDIDO — HORA — CADUCA

ABG.FEY BRIGIS REYOREGO

Jefa del Registro Judicial de la Nación
GERENCIA GENERAL
SISTEMA JUDICIAL

Página 1 de 1 — La información en el presente certificado, puede ser verificada vía internet, en la siguiente dirección http://scertss.pj.gob.pe/cap
Con el código: [redacted]

Fuente: DGTAIPD del Minjusdh



Fuente: DGTAIPD del Minjusdh

¡RECUERDA!

- **Se debe tener presente que la aplicación** del procedimiento de anonimización no depende del tipo de documento o archivo digital en el que se encuentren contenidos los datos personales, sino, como se ha señalado, depende de la finalidad del tratamiento que se les dará (ya sea para su entrega o publicación). En ese sentido, cuando corresponda eliminar los datos de forma tal que el titular no pueda ser reidentificado, la entidad pública deberá aplicar dicho procedimiento.

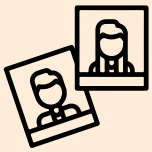
6.2.2. Anonimización para datos no estructurados relacionados a imágenes, videos, datos biométricos o grabaciones de audio

La anonimización de datos personales no estructurados se refiere al conjunto de técnicas destinadas a suprimir, alterar o transformar elementos identificables contenidos en archivos de naturaleza distinta al texto —como imágenes, videos, grabaciones de audio o datos biométricos— con el propósito de impedir la reidentificación de los titulares. Este tipo de información presenta un grado superior de complejidad, dado que en muchos casos el propio archivo constituye el dato personal. Un ejemplo evidente es la voz: una grabación de audio no solo contiene información expresada verbalmente, sino que el propio archivo de audio puede considerarse un dato personal en sí mismo.

Por otro lado, debido a la naturaleza de los datos no estructurados, muchas veces es necesario emplear sistemas de información especializados que permitan la aplicación de las técnicas apropiadas.

La determinación de la razonabilidad respecto a la posibilidad de reidentificación del titular del dato personal recae en la entidad pública que aplica el procedimiento de anonimización, por lo que se recomienda extrema cautela al divulgar, difundir o entregar información en cualquier formato que haga referencia a datos no estructurados relacionados a imágenes, videos, datos biométricos o grabaciones de audio.

EJEMPLO DE LA APLICACIÓN DE LA ANONIMIZACIÓN PARA ESTE TIPO DE DATOS NO ESTRUCTURADOS SE DETALLA A CONTINUACIÓN:



Para imágenes: En fotografías o documentos escaneados, la anonimización se logra mediante técnicas como el desenfoque, el pixelado o la cobertura de zonas específicas (rostros, direcciones visibles, etc.).

Ejemplo: una fotografía utilizada en un informe público de actividades comunitarias, donde se difumina el rostro de los menores de edad presentes.

Para videos: La anonimización en material audiovisual combina la necesidad de preservar el valor informativo del contenido con la supresión de elementos identificativos. Se emplean métodos como la distorsión de imágenes en movimiento (en rostros o direcciones) y la modificación del audio en paralelo.

Ejemplo: un video de seguridad vial publicado para fines de conocimiento público, en el cual se distorsionan los rostros de peatones y conductores.

Para grabaciones de audio: En este ámbito, la voz constituye un identificador biométrico. La anonimización requiere aplicar transformaciones irreversibles como la alteración del timbre, la velocidad o el tono de la grabación, de forma que se conserve el contenido semántico pero sin posibilidad de reconocer al hablante.

Ejemplo: una entrevista de carácter cualitativo difundida en un portal académico, donde se distorsiona la voz de los entrevistados para garantizar su anonimato.

En todos los casos, la característica esencial es la irreversibilidad razonable del procedimiento: las técnicas aplicadas deben impedir que un tercero, incluso con acceso a herramientas tecnológicas avanzadas o a información adicional, pueda restituir los atributos originales o identificar al titular de los datos. De este modo, la anonimización de datos no estructurados permite compatibilizar la finalidad de transparencia, investigación o difusión de información pública, con el cumplimiento de los principios de confidencialidad y seguridad en el tratamiento de datos personales.

7

Técnica recomendada para la conservación, almacenamiento y tránsito seguro de información que contiene datos personales: Seudonimización

7 Técnica recomendada para la conservación, almacenamiento y tránsito seguro de información que contiene datos personales: Seudonimización

La seudonimización constituye una técnica de protección de datos personales que tiene como finalidad garantizar el almacenamiento, conservación y tránsito seguro de la información, reduciendo el riesgo de exposición en caso de accesos no autorizados o exfiltración de la información seudonimizada. No obstante, a diferencia de la disociación y anonimización, la seudonimización no se aplica para la entrega y/o publicación de información al público, sino para el manejo interno de bases de datos y sistemas de información donde se requiere preservar la operatividad del dato sin exponerlo directamente.

Cabe señalar que, si bien la aplicación de mecanismos de seudonimización como medida de seguridad sobre datos personales puede dificultar la reidentificación del titular en determinados contextos, esta característica no debe confundirse con la finalidad propia de los mecanismos de disociación o anonimización. Ello se debe a que los datos seudonimizados están diseñados para permitir, en el marco adecuado y bajo condiciones de seguridad, la reconstrucción del dato original (en el caso de la aplicación de algoritmos de cifrado bidireccional) o la verificación de la integridad de la información (en el caso de la aplicación de funciones criptográficas HASH)

7.1. Seudonimización por aplicación de algoritmos de cifrado:

Definición

Consiste en aplicar algoritmos criptográficos que convierten un dato personal en un valor cifrado (ilegible) que solo puede ser revertido a su forma original mediante la clave de cifrado correspondiente. Se emplea en contextos donde la entidad (a través de un sistema de información) necesita recuperar el dato original, como en procesos administrativos, pagos o verificaciones de identidad

Ejemplo 1:

El Portal de Servicios al Ciudadano de una entidad pública permite a los beneficiarios generar cuentas de usuario para consultar el estado de sus trámites y acceder a subsidios. En este contexto, la entidad considera almacenar los números de DNI de los ciudadanos aplicando la seudonimización mediante cifrado bidireccional con el fin de reducir los riesgos de exposición de datos personales. La finalidad es garantizar que el DNI solo pueda ser accedido en circunstancias estrictamente necesarias y bajo control, manteniéndolo cifrado en reposo y en tránsito.

El ciudadano crea su cuenta en la plataforma estatal, ingresando su DNI, contraseña y demás datos personales en un formulario. El sistema no almacena el número de DNI en texto plano. En su lugar, se aplica un algoritmo de cifrado seguro (ej. AES-256 en modo CBC, con clave gestionada en un Módulo de Seguridad Hardware – HSM administrado por el Centro Nacional de Seguridad Digital). Como resultado, la base de datos de la entidad conserva únicamente el DNI cifrado, junto con un identificador interno para operar en los procesos rutinarios.

En este escenario, el número de DNI puede ser descifrado únicamente bajo un contexto autorizado (p. ej., validación en el proceso de pago de subsidios o en la verificación contra RENIEC). Esto asegura que la entidad estatal mantenga control sobre los accesos y que el dato personal no pueda ser interpretado sin las claves seguras, mientras se cumple con los principios de confidencialidad y minimización establecidos por la LPDP y su RLPDP.

7.2. Seudonimización por aplicación de función criptográfica hash:

Definición

Técnica que consiste en emplear una función HASH (algoritmo criptográfico unidireccional) para encriptar el dato personal conservar, almacenar y/o publicar, dando como resultado una cadena de caracteres única de longitud fija (valor hash).

Esta técnica se caracteriza porque genera una especie de huella digital del dato original y hace imposible matemáticamente reconstruirlo partiendo de la dicha huella (valor hash)

Sin embargo, si el dato personal que ha sido hasheado pertenece a un conjunto predecible de valores, como un número de DNI (del cual se conoce su estructura), es técnicamente posible para un atacante aplicar la función HASH sobre un diccionario de todos los DNI existentes (fuerza bruta) y, cuando el resultado obtenido por el atacante coincida con el publicado por la entidad, este confirmará el dato personal original.

Ejemplo:

El Portal de Servicios al Ciudadano de una entidad pública permite a los beneficiarios generar cuentas de usuario para consultar el estado de sus trámites y acceder a subsidios. En este contexto, la entidad considera almacenar las contraseñas de los ciudadanos aplicando la seudonimización mediante función criptográfica HASH (unidireccional) con el fin de

protegerlas. La finalidad es garantizar que no puedan ser recuperadas ni visualizadas, sino únicamente verificadas en el momento de la autenticación.

El ciudadano crea su cuenta en la plataforma estatal, ingresando su DNI y una contraseña en el formulario. El sistema no almacena la contraseña en claro. En su lugar, se aplica una función de derivación segura (ej. Argon2id, recomendada por el Centro Nacional de Seguridad Digital). Como resultado, la base de datos de la entidad conserva un hash de la contraseña.

Posteriormente, cuando el ciudadano requiera iniciar sesión en el Portal de Servicios al Ciudadano, este introduce su contraseña. A continuación, el sistema repite la función de derivación y genera un nuevo hash de contraseña. Este se compara con el valor almacenado, si coincide, el Portal de Servicios al Ciudadano permite el acceso al ciudadano, caso contrario, el acceso es denegado.

En ningún momento la contraseña en texto plano es visible ni al personal de la entidad ni a los administradores de la base de datos.

En este escenario, lo único que puede realizarse es validar si una contraseña propuesta corresponde al hash guardado. Esto asegura que ni la propia entidad estatal ni un atacante con acceso a la base de datos pueda reconstruir las contraseñas.

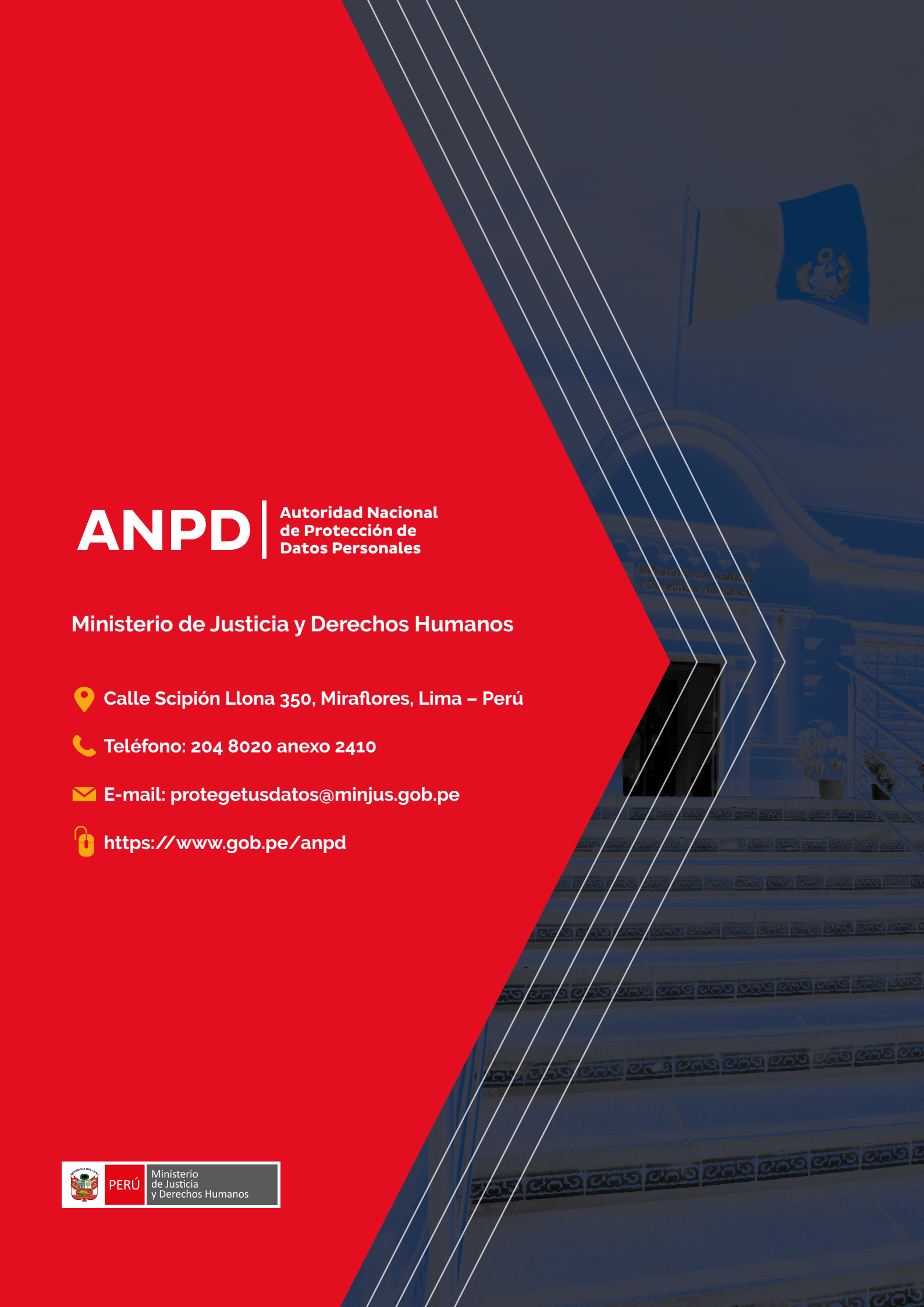
ANEXO: OPINIONES CONSULTIVAS SOBRE DISOCIACION Y ANONIMIZACION DE DATOS PERSONALES

A efectos de una mejor comprensión, la Dirección General que ejerce las ANPD y la ANTAIP ha emitido opiniones consultivas en las que se establece la aplicación de disociación y anonimización en diversos supuestos. A continuación, se detalla lo señalado.

Opiniones consultivas emitidas:

Opinión Consultiva	Fecha	LINK	Asunto
Opinión Consultiva N.° 59-2018-JUS/ DGTAIPD	12/11/2018	https://shre.ink/tQUl	Publicación de resoluciones que ponen término al procedimiento administrativo sancionador por responsabilidad administrativa funcionarial
Opinión Consultiva N.° 21-2019-JUS/ DGTAIPD	13/02/2019	https://shre.ink/tQUr	Sobre la publicidad y la máxima divulgación de la información del Estado
Opinión Consultiva N.° 37-2019-JUS/ DGTAIPD	26/06/2019	https://shre.ink/tQUQ	Sobre el acceso de los datos personales de los funcionarios públicos a través de las solicitudes de acceso a la información pública
Opinión Consultiva N.° 09-2020-JUS/ DGTAIPD	17/01/2020	https://shre.ink/tQU9	Sobre la protección de los datos personales del funcionario, contenidos en la información vinculada el ejercicio de la potestad sancionadora disciplinaria de la administración pública
Opinión Consultiva N.° 11-2020-JUS/ DGTAIPD	03/02/2020	https://shre.ink/tQn4	Sobre publicidad de la relación de adherentes presentada para certificación de autenticidad de firmas, a propósito de una eventual demanda de inconstitucionalidad
Opinión Consultiva N.° 44-2020-JUS/ DGTAIPD	30/10/2020	https://shre.ink/tQnw	Acceso a la información de titulares de un contrato de suministro de prestación de servicios públicos
Opinión Consultiva N.° 41-2022-JUS/ DGTAIPD	12/12/2022	https://shre.ink/tQnR	Sobre requerimiento de historia clínica por parte de un Tribunal Arbitral
Opinión Consultiva N.° 07-2023-JUS/ DGTAIPD	03/02/2023	https://shre.ink/tQni	Entrega de boletas de pago en el marco de un procedimiento de negociación colectiva
Opinión Consultiva N.° 22-2023-JUS/ DGTAIPD	07/07/2023	https://shre.ink/tQnu	Sobre la protección de datos personales contenidos en el Padrón General de Hogares y el acceso de las entidades públicas a la información de la clasificación socioeconómica – CSE
Opinión Consultiva N.° 12-2024-JUS/ DGTAIPD	01/07/2024	https://shre.ink/tQn7	Sobre entrega de video y documentos de postulante en el marco de un concurso de méritos
Opinión Consultiva N.° 08-2025-JUS/ DGTAIPD	28/01/2025	https://shre.ink/tQn5	Opinión acerca de la transferencia de datos al Centro de Epidemiología, Prevención y Control de Enfermedades para la implementación del Registro Nacional de Cáncer

Fuente: DGTAIPD del Minjusdh



ANPD | Autoridad Nacional de Protección de Datos Personales

Ministerio de Justicia y Derechos Humanos

Calle Scipión Llona 350, Miraflores, Lima – Perú

Teléfono: 204 8020 anexo 2410

E-mail: protegetusdatos@minjus.gob.pe

https://www.gob.pe/anpd

PERÚ | Ministerio de Justicia y Derechos Humanos