# GUÍA PARA LA DISOCIACIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

**INSTITUTO DE TRANSPARENCIA, INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE JALISCO**

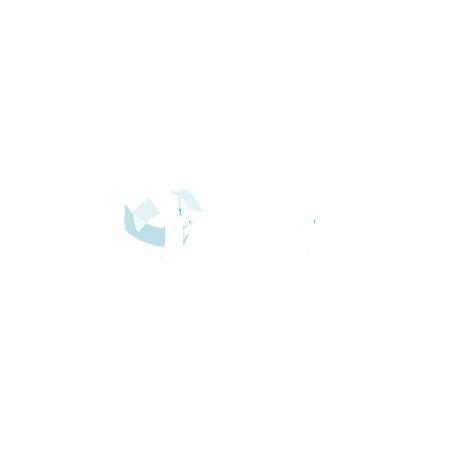


Imagen que contiene persona, cadena, frente, sostener

Descripción generada automáticamente

# DIRECTORIO

**Cynthia Patricia Cantero Pacheco**

Comisionada Presidenta

**Salvador Romero Espinosa**

Comisionado Ciudadano

**Pedro Antonio Rosas Hernández**

Comisionado Ciudadano

**Miguel Ángel Hernández Velázquez**

Secretario Ejecutivo

**Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, Abril 2020.**

**Avenida Vallarta 1312 colonia Americana C.P. 44160 Guadalajara, Jalisco, México.**

**Tel. (33) 3630 5745**

# CONTENIDO

[DIRECTORIO 2](#_Toc38285044)

[CONTENIDO 3](#_Toc38285045)

[GLOSARIO 4](#_Toc38285046)

[I.INTRODUCCIÓN 5](#_Toc38285047)

[II. MARCO NORMATIVO 6](#_Toc38285048)

[1. ETAPAS DEL PROCESO DE DISOCIACIÓN 7](#_Toc38285049)

[1.1 DISEÑO DEL PROYECTO 7](#_Toc38285050)

[1.1.1 CLASIFICACIÓN DE LOS DATOS PERSONALES 7](#_Toc38285051)

[a) Datos personales 7](#_Toc38285052)

[b) Datos personales sensibles 9](#_Toc38285053)

[1.1.2 IDENTIFICACIÓN DE INFORMACIÓN 9](#_Toc38285054)

[1.2 DISOCIACIÓN 10](#_Toc38285055)

[1.2.1 TÉCNICAS DE DISOCIACIÓN 10](#_Toc38285056)

[1.2.1.1 ALEATORIZACIÓN 10](#_Toc38285057)

[a) Adición de ruido 11](#_Toc38285058)

[b) Permutación 11](#_Toc38285059)

[c) Privacidad diferencial 11](#_Toc38285060)

[1.2.1.2 GENERALIZACIÓN 12](#_Toc38285061)

[1.2.1.3 SUPRESIÓN 12](#_Toc38285062)

[1.3 CONTROL 14](#_Toc38285063)

[2. RESUMEN 15](#_Toc38285064)

[3. REFERENCIAS 16](#_Toc38285065)

# GLOSARIO

**Criterio de minimización:** El responsable procurará realizar esfuerzos razonables para tratar los datos personales al mínimo necesario, con relación a las finalidades que motivan su tratamiento.

**Dato personal:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

**Datos sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

**Disociación:** El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

**Titular:** Persona física a quien pertenecen los datos personales.

**Tratamiento:** De manera enunciativa más no limitativa cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

# I. INTRODUCCIÓN

Es ampliamente conocido que con los avances tecnológicos es más fácil y rápido obtener información. Los entes públicos, en el ejercicio de sus funciones recaban, manejan y generan datos personales relativos a su personal y a la ciudadanía con la que tienen algún tipo de relación jurídica.

Es por ello que, se ha implementado normativa para definir los límites que como tales se tienen con respecto al uso de los datos personales, ya que los datos que se recaban y el tratamiento que se les da es diverso y distinto según quien realiza la actividad de acuerdo a su ámbito de competencia y atribuciones (gobierno federal, estatal y municipal).

Con los temas de transparencia y acceso a la información pública, la ciudadanía ha comenzado a tener especial interés en conocer la información que se encuentra en poder del Estado, ya que esta puede ser utilizada en beneficio de la sociedad, especialmente a través de los datos abiertos, razón por la que es imperativo tomar las precauciones necesarias a fin de evitar algún tipo de vulneración o riesgo de vulnerar los datos personales de los titulares en poder de cada sujeto obligado responsable.

A través de este documento, el Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, por conducto de su Dirección de Protección de Datos Personales, ha desarrollado una serie de pasos y técnicas a fin de que los sujetos obligados del estado, en su carácter de responsables, tengan las herramientas necesarias para disminuir el riesgo de re- identificación de aquellos titulares cuyos datos personales se encuentran en resguardo de estos entes públicos a través de un efectivo proceso de disociación.

Hay que tomar en cuenta que, con los avances tecnológicos, el proceso de disociación debe ser monitoreando, actualizando y modificando constantemente a fin de que no resulte obsoleto y se genere un riesgo para los titulares de los datos.

# II. MARCO NORMATIVO

En principio, es preciso aclarar que si bien a todos los sujetos obligados del Estado de Jalisco les es aplicable tanto la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en lo sucesivo Ley General), como la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios (en lo sucesivo Ley Estatal), para cada sujeto obligado resulta diferente el ordenamiento legal que les faculta para recabar y tratar datos personales.

Razón por la cual, cada uno deberá atender a las normas, leyes, reglamentos y/o decretos que les dan vida, así como aquellas que les otorgan atribuciones y facultades que rigen su actuar diario, ya que son estas las que les permiten recabar y tratar datos personales.

Ahora bien, la ley Estatal en su artículo 15 fracción VII, señala como otra excepción al consentimiento, el previo sometimiento de estos a un procedimiento de disociación.

Atendiendo a lo anterior, los datos personales deben tratarse de un modo que garantice su seguridad y confidencialidad adecuadas, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo tecnológico utilizado en el tratamiento.

# 1. ETAPAS DEL PROCESO DE DISOCIACIÓN

En el ámbito de la protección de los datos personales hay que tomar en cuenta que existen datos personales relativos a personas identificadas, es decir, aquellos cuya vinculación con el titular no ha sido eliminada u oculta; existen datos relativos a personas identificables, es decir, datos que no se asocian directamente a un titular determinado, ya que el titular no está identificado o no hay vínculo entre la persona y el dato, sin embargo, es fácil que tras algún procedimiento se pueda identificar al titular; los datos anónimos, es decir, aquellos datos que han sido recabados sin vincularlos desde un inicio con su titular y; los datos anonimizados, es decir, los que han sido sometidos a un proceso de disociación efectivo, por lo que la identidad del titular no es conocida y es imposible su identificación.

Los datos personales se deben obtener y tratar de conformidad con la legislación aplicable vigente al sujeto obligado, el proceso de disociación, resulta ser un tratamiento posterior a la obtención de los datos personales, por lo cual se deberá cumplir con el principio de finalidad establecido en el artículo 11 de la Ley Estatal.

## 1.1 DISEÑO DEL PROYECTO

En esta etapa los responsables deberán identificar con claridad los datos personales que se recaban por categoría, los datos confidenciales, la o las técnicas a implementar para la disociación, el riesgo de re- identificación asociado y la ejecución del proyecto.

Se deberán definir de manera clara y específica los perfiles del quienes participaran del proceso de disociación; es decir, los usuarios, los técnicos informáticos, el titular la unidad de transparencia o en su caso el oficial de protección de datos personales.

## 1.1.1 CLASIFICACIÓN DE LOS DATOS PERSONALES

## a) Datos personales

Dato personal es cualquier información concerniente a una persona física identificada o identificable; se considera que una persona es identificable, cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.[[1]](#footnote-1)

**DATOS DE IDENTIFICACIÓN Y CONTACTO**

Nombre, estado civil, número de matrícula, registro federal de contribuyentes (RFC), clave única de registro de población (CURP), clave de elector, matrícula del servicio militar nacional, número de pasaporte, lugar de nacimiento, fecha de nacimiento, nacionalidad, domicilio, teléfono particular, teléfono celular, correo electrónico, número de afiliación al seguro social, seudónimo, apodo, nombre de usuario en redes sociales, firma autógrafa, firma electrónica, edad, fotografía, referencias personales, dirección IP, número de serie de celular.

**DATOS SOBRE CARACTERÍSTICAS FÍSICAS**

Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, cicatrices, tipo de sangre, tatuajes, perforaciones, complexión física.

**BIOMÉTRICOS**

Huella dactilar, geometría de la mano (las curvas de los dedos, su grosor y longitud, la altura y la anchura del dorso de la mano, las distancias entre las articulaciones y la estructura ósea), reconocimiento facial, reconocimiento de iris, reconocimiento de retina, reconocimiento vascular, reconocimiento de firma autógrafa o manuscrita, reconocimiento de escritura, reconocimiento de voz, reconocimiento de escritura de teclado, reconocimiento de la forma de andar (Se encuentra aún en desarrollo y no tiene los mismos niveles de rendimiento que otras tecnologías biométricas).

**LABORALES**

Puesto o cargo que desempeña, nombramientos, incidencia, actividades extracurriculares, solicitud de empleo, hoja de servicio, domicilio de trabajo, correo electrónico institucional, teléfono institucional, referencias laborales, información generada durante los procedimientos de reclutamiento, selección y contratación, experiencia, capacitación laboral.

**ACADÉMICOS**

Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados, reconocimientos.

**MIGRATORIOS**

Entrada al país, salida del país, tiempo de permanencia en el país, calidad migratoria, derechos de residencia, aseguramiento, repatriación.

**PATRIMONIALES/FINANCIEROS**

Bienes muebles, bienes inmuebles, información fiscal, historial crediticio, buró de crédito, ingresos, egresos, cuentas bancarias, números de tarjetas de crédito, información adicional de tarjeta (fecha de vencimiento, códigos de seguridad, datos de banda magnética, pin), seguros, fianza, servicios contratados, referencias personales, afores.

**PASATIEMPOS**

Deportes que practica, juegos de su interés, actividad artística, música de interés, libros de interés, programas de televisión de interés, películas de interés, actividades al aire libre.

**PROCEDIMIENTOS ADMINISTRATIVOS Y/O JURISDICCIONALES**

La información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho.

## b) Datos personales sensibles

Son datos personales sensibles aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.[[2]](#footnote-2)

**IDEOLÓGICOS**

Religión, Afiliación ó ideología política, creencias o convicción filosófica.

**DE SALUD**

Estado de salud física presente, pasado o futuro, estado de salud mental presente, pasado o futuro, razones de hospitalización, expediente clínico, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, uso de aparatos ortopédicos, uso de aparatos auditivos, uso de prótesis, Información genética, vida sexual.

**PREFERENCIAS SEXUALES**

**DATOS DE ORÍGEN ÉTNICO/RACIAL**

## 1.1.2 IDENTIFICACIÓN DE INFORMACIÓN

Una vez identificados y clasificados los datos personales recabados por el sujeto obligado, se deberá seleccionar aquella información que será incluida en el proceso de disociación, esto debido a que no toda la información que posee el sujeto obligado responsable es susceptible de ser publicada en formato abierto, ejemplo de esto son tanto la información confidencial como la información reservada[[3]](#footnote-3).

Para lograr un análisis efectivo hay que tomar en cuenta y aplicar correctamente el criterio de minimización; es decir, hay que recabar los datos personales que resulten mínimamente necesarios para las finalidades específicas del sujeto obligado, de esta manera serán mínimos los datos personales existentes dentro del conjunto de datos a tratar y por ende será menor la cantidad de información personal en posesión del responsable y será más sencillo llevar a cabo el procedimiento de disociación.

Se deberá tener presente que, para el caso de datos personales sensibles, se requiere un mayor cuidado con la finalidad de evitar que el proceso de disociación pueda ser revertido, por lo que se debe analizar la necesidad real e indispensable de utilizar dicha información.

## 1.2 DISOCIACIÓN

Procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.[[4]](#footnote-4) Es una herramienta utilizada para aquellos casos en que se van a utilizar datos personales de manera masiva, cuando se van a utilizar los datos para estudios, estadísticas, versiones públicas de bases de datos; por nombrar algunos casos.

Un ejemplo de uso de datos de manera masiva serían los datos personales que recaba el [Instituto Nacional de Estadística y Geografía (INEGI)](https://www.inegi.org.mx/) al llevar a cabo los censos de población, aplica técnicas de disociación, para finalmente, presentar solamente estadísticas de los datos previamente recabados, de tal manera que es imposible identificar al titular de cada dato de los presentados por el INEGI.

Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento; sin embargo, se debe considerar que, con respecto a los datos personales seleccionados para su disociación, en todo momento se debe atender al caso concreto, esto debido a que en algunos casos no es suficiente aplicar una técnica de disociación, sino que resulta necesario aplicar más de una a fin de garantizar la no identificación del titular de los datos personales.

## 1.2.1 TÉCNICAS DE DISOCIACIÓN

Una vez seleccionados los datos personales que serán sometidos al procedimiento de disociación, el responsable deberá elegir la o las técnicas pertinentes para lograr dicho procedimiento, atendiendo siempre al tipo de datos que se están tratando, el número de titulares y el factor de riesgo (su gravedad, la probabilidad del riesgo, las consecuencias para el responsable y el titular).

Por ello, se recomienda que atendiendo al caso concreto se determine si se aplica una técnica o más de una para garantizar que no se pueda re- identificar al titular y evitar un riesgo.

Para que los datos puedan ser utilizados en un formato abierto, la disociación deberá garantizar que no se pueda establecer un vínculo de ningún tipo entre el dato personal y su titular, o al menos esto deberá representar un esfuerzo desproporcionado; ya que de ser así, se deberá buscar la anonimidad completa los datos personales.

Un efectivo procedimiento de disociación no puede ser reversible, siendo el equivale a un borrado permanente.

## 1.2.1.1 ALEATORIZACIÓN

Consiste en un conjunto de técnicas cuyo objetivo es el de modificar la veracidad del dato con la finalidad de suprimir el vínculo que existe entre este y su titular, volviendo los datos lo suficientemente ambiguos para evitar que se identifique a una persona concreta, sin que se pierda la certeza y utilidad de la información que se proporciona.

Dentro de esta técnica encontramos dos tipos:

## a) Adición de ruido

Es una técnica complementaria, se emplea modificando los atributos del conjunto de datos personales a fin de que resulten ser menos exactos, pero se conserva la atribución general, resultado de ello, los datos son ciertos hasta determinados puntos.

Un ejemplo de ello es cuando se tiene información de una persona con una edad de 30 años, se agregan valores de -10 años y de + 10 años, lo que se reflejaría al momento de presentar la información como que se tiene información de una persona con una edad de los 20 a los 40 años, haciendo difícil identificar a aquella persona que tiene 30 años.

Es recomendable combinar esta técnica con otras a fin de hacer más efectivo el procedimiento de disociación, ya que la adición de ruido puede tener errores y defectos.

## b) Permutación

Esta técnica consiste en mezclar los valores de los atributos en una tabla para que algunos de ellos puedan vincularse artificialmente a distintos titulares; en otras palabras, se intercambian algunos valores de un conjunto de datos con los de otro conjunto de datos, sin romper la relación lógica y la veracidad de la información.

Es recomendable combinar esta técnica con otras a fin de hacer más efectivo el procedimiento de disociación.

## c) Privacidad diferencial

En esta técnica, se toman los datos personales de la totalidad de los titulares a los que se les recabe dicha información, sin saber a quién corresponde cada dato; es decir, el responsable genera vistas anonimizadas del conjunto de datos, pero al mismo tiempo almacena copias de los originales para que únicamente el responsable pueda identificar a los titulares a partir de los resultados de las consultas de privacidad diferencial, resultados que deben considerarse como datos personales a los cuales se debe aplicar la normativa vigente en la materia.

Es recomendable que además de esta técnica se añada ruido en los resultados de las consultas, a fin de garantizar que no se pueda re- identificar a los titulares.

## 1.2.1.2 GENERALIZACIÓN

Mediante esta técnica, se modifican las escalas u órdenes de magnitud; es decir, se descarta la singularización que en conjunto con otras técnicas impiden la vinculación del dato personal con el titular de este. Puede ser mediante agrupar los datos de un titular con un determinado número de personas, es decir, mediante agregación y anonimato K.

Ejemplo de ello es cuando se tiene un grupo de personas con edades variadas, las cuales se pretende no sean conocidas con exactitud porque representaría un riesgo para sus titulares, por lo que, el responsable agrupa las edades para formar intervalos de valores, es decir, en lugar de mostrar las edades específicas de los titulares, se separan las edades por grupos y se separan por grupos de edad y se señalan intervalos: 18, 22, 37, 19, 40, 55, 36, 44, 60

|  |  |
| --- | --- |
| Edad: | Edad |
| 18, 19 | menos de 20 años |
| 22 | 20- 30 |
| 37, 40, 36 | 30- 40 |
| 44 | 40- 50 |
| 55, 60 | 50- 60 |

## 1.2.1.3 SUPRESIÓN

Se reemplazan los datos personales con asteriscos, a fin de señalar que se tiene el dato, pero se está omitiendo por seguridad de su titular.

Por ejemplo, en la siguiente tabla se encuentran los datos personales tal cual se recaban:

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Edad** | **Municipio** | **Género** |
| Juan Pérez | 44 | TONALÁ | M |
| María Elena Gómez | 40 | ZAPOPAN | F |
| José Francisco Hernández | 22 | GUADALAJARA | M |
| Jorge Alberto Martínez | 37 | ZAPOPAN | M |

En la tabla siguiente se han suprimido algunos datos, por lo que es más complicado determinar quién es el titular de estos:

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Edad** | **Municipio** | **Género** |
| Juan \*\* | \*4 | TONALÁ | M |
| \*\* | 40 | ZAPOPAN | F |
| José \*\* | \*2 | GUADALAJARA | M |
| \*\* | 37 | ZAPOPAN | M |

Esta técnica se suele combinar con la de generalización para una disociación efectiva.

Si en distintas áreas del mismo sujeto obligado responsable se manejan distintos datos pertenecientes al mismo titular, se deberán implementar las técnicas de disociación necesarias, de tal manera que, si alguien tiene acceso a la información de dichas áreas, no pueda empatar la misma y no pueda por inferencia identificar al titular.

En una empresa, en dos áreas diferentes, tienen la siguiente información de sus empleados:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nombre** | **Edad** | **Municipio** | **Género** | **Número de empleado** | **Cargo** |
| Juan Pérez | 44 | TONALÁ | M | 065 | Coordinador |
| María Elena Gómez | 40 | ZAPOPAN | F | 072 | Secretaria |
| José Francisco Hernández | 22 | GUADALAJARA | M | 044 | Director General |
| Jorge Alberto Martínez | 37 | ZAPOPAN | M | 093 | Coordinador |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Número de empleado** | **Edad** | **Fecha de Nacimiento** | **Municipio** | **Género** | **Cargo** |
| 065 | 44 | 1976 | TONALÁ | M | Coordinador de calidad |
| 072 | 40 | 1980 | ZAPOPAN | F | Secretaria de dirección |
| 044 | 22 | 1998 | GUADALAJARA | M | Director General “A” |
| 093 | 37 | 1983 | ZAPOPAN | M | Coordinador “A” |

El responsable de cada área utilizó una o varias técnicas de disociación, a fin de que los titulares no sean identificables, resultando el siguiente ejemplo:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nombre** | **Edad** | **Región Administrativa del Estado de Jalisco** | **Género** | **Número de empleado** | **Cargo** |
| \*\* | De los 40 a los 50 años | Región XII Centro | M | 065 | Coordinador |
| \*\* | De los 30 a los 40 años | Región XII Centro | F | 072 | Secretaria |
| \*\* | De los 20 a los treinta años | Región XII Centro | M | 044 | Director General |
| \*\* | De los 30 a los 40 años | Región XII Centro | M | 093 | Coordinador |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Número de empleado** | **Edad** | **Fecha de Nacimiento** | **Región Administrativa del Estado de Jalisco** | **Género** | **Cargo** |
| 0\*5 | De los 40 a los 50 años | Entre 1970 y 1980 | Región XII Centro | M | Coordinador |
| 0\*2 | De los 30 a los 40 años | Entre 1970 y 1980 | Región XII Centro | F | Secretaria |
| 0\*4 | De los 20 a los treinta años | Entre 1990 y 2000 | Región XII Centro | M | Director General |
| 0\*3 | De los 30 a los 40 años | Entre 1980 y 1990 | Región XII Centro | M | Coordinador |

## 1.3 CONTROL

Es la tercera fase del proceso de disociación, esta etapa se debe realizar periódicamente, especialmente si surgen nuevas tecnologías o técnicas para prevenir y evitar los posibles riesgos de re- identificación.

Se debe analizar si la o las técnicas implementadas para la disociación pueden ser reversibles o a pesar de ellas podría re- identificarse al titular de estos, en cuyo caso es recomendable dar de baja al conjunto de datos o implementar nuevas técnicas.

Es recomendable realizar un proceso de control a la disociación de los datos personales, información reservada o confidencial del responsable, mínimo 3 veces por año calendario, detectando cuales fueron las técnicas utilizadas y si estas siguen vigentes.

# 2. RESUMEN / RUTA CRITICA

DISEÑO DEL PROYECTO

* Actores
* Clasificación de los datos personales recabados
* Identificación de los datos personales a someter al proceso

DISOCIACIÓN

Analizar la eficacia de las técnicas de disociación implementadas para discernir si es necesario implementar nuevas o suprimir los datos

CONTROL

* Aleatorización
* Generalización
* Supresión

# 3. REFERENCIAS

Agencia española de protección de datos personales. (abril de 2020). *La K-Anonimidad como medida de la privacidad.* Madrid, España. Recuperado el marzo, abril de 2020, de Agencia española de protección de datos personales: https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-kanonimidad.pdf

AGESIC. (diciembre de 2017). *Guía de disociación y anonimización de datos personales en el ámbito de la salud.* Montevideo. Recuperado el marzo, abril de 2020, de Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Infromación y el Conocimiento: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2018). *Guía para el Tratamiento de Datos Biométricos.* Recuperado el marzo, abril de 2020, de http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos\_Web\_Links.pdf

ITEI. (2014). *LINEAMIENTOS GENERALES PARA LA PROTECCiÓN DE LA INFORMACiÓN CONFIDENCIAL Y RESERVADA QUE DEBERÁN OBSERVAR LOS SUJETOS OBLIGADOS PREVISTOS EN LA LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DEL ESTADO DE JALISCO Y SUS MUNICIPIOS.* Recuperado el marzo, abril de 2020, de https://www.itei.org.mx/v4/index.php/normatividad

1. Artículo 3 fracción IX de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios [↑](#footnote-ref-1)
2. Artículo 3 fracción X de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios [↑](#footnote-ref-2)
3. Artículos 21 y 17 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios [↑](#footnote-ref-3)
4. Artículo 3° fracción XIII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios. [↑](#footnote-ref-4)