MANUAL DE PROTECCIÓN DE DATOS PERSONALES

Adjuntía en Asuntos Constitucionales

Defensoría del Pueblo

MANUAL DE PROTECCIÓN DE DATOS PERSONALES

Adjuntía en Asuntos Constitucionales

Lima, noviembre 2019

Defensoría del Pueblo
Jirón Ucayali Nº 394-398
Lima 1, Perú
Teléfono: (511) 311- 0300
Fax: (511) 426 -7889
E-mail: consulta@defensoria.gob.pe
Web: www.defensoria.gob.pe
Twitter: @Defensoria_Peru
Línea gratuita: 0800-15170

Primera edición: Lima, noviembre del 2019
Hecho el Depósito Legal en la Biblioteca Nacional del Perú N° 2019 - 15295

Edición y Diseño: Jasmin Luisa Pablo Falconí
Impresión: IMPREXPERU - Romulo Herrera Llerena

Este manual ha sido elaborado por la Adjuntía en Asuntos Constitucionales. La investigación y redacción estuvo a cargo de Karina Díaz Farroñay y Silvana Escudero Casanova, bajo la dirección de Abraham García Chávarri, Adjunto (e) en Asuntos Constitucionales.

La elaboración del presente manual contó con el apoyo de Rosa Ataurima Castillo y Rina Palacios Esterripa.

LA DEFENSORÍA DEL PUEBLO EN DEFENSA DE TUS DERECHOS ...

CONTENIDO

PRESENTACIÓN 9

LOS DATOS PERSONALES

1.- ¿Qué son los Datos Personales? 10
2.- ¿Por qué proteger los Datos Personales? 11
3.- ¿Qué normas protegen los Datos Personales en el Perú?
4.- ¿Cómo proteger los Datos Personales? 12
5.- ¿Cuáles son los principios que guían el uso de Datos Personales? 13

TRATAMIENTO DE DATOS PERSONALES

6.- ¿En qué consiste el tratamiento de Datos Personales? 14
7.- ¿Qué es el consentimiento para el tratamiento de Datos Personales?
8.- ¿Cuándo no se requiere consentimiento? 15
9.- ¿En qué consiste el flujo transfronterizo de datos? 17
10.- ¿Cómo brindar seguridad al tratamiento de Datos Personales?
11.- ¿Cómo proteger la confidencialidad en el tratamiento de Datos Personales? 18

DERECHOS DEL TITULAR DE DATOS PERSONALES

12.- ¿Qué son los derechos "ARCO"? 19
13.- ¿Qué otros derechos tiene el titular de Datos Personales? 20

OBLIGACIONES DEL TITULAR Y ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES

14.- ¿Qué son los bancos de Datos Personales? 21
15.- ¿Quién es el titular y el encargado del tratamiento de Datos Personales? 22
16.- ¿Qué obligaciones tiene el titular y el encargado del tratamiento de Datos Personales?

AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

17.- ¿Qué es la Autoridad Nacional de Protección de Datos Personales? 23
18.- ¿Cuáles son las funciones de la Autoridad Nacional de Protección de Datos Personales?
19.- ¿En qué consiste el procedimiento trilateral de tutela? 25
20.- ¿En qué consiste la facultad sancionadora de la Autoridad? 27

SOBRE ESTA EDICIÓN 30

ENCUESTA 32

REFERENCIAS 33

PRESENTACIÓN

Los datos personales son toda aquella información que permite identificarnos o nos hace identificables, como el nombre, el domicilio, la imagen u otros, por lo que tienen una directa e íntima relación con las distintas actividades que desarrollamos en nuestra vida diaria. Su protección deviene, por ello, en indispensable.

Cuando contratamos servicios de agua o luz, damos nuestro documento de identidad y señalamos nuestro domicilio; cuando adquirimos productos mediante el uso de tarjetas de crédito, firmamos para autorizar la transacción; cuando solicitamos un producto por delivery, brindamos el celular y la dirección de destino; incluso, cuando nos registramos en alguna red social o descargamos una app entregamos datos de identificación.

De allí y ante la preocupación que existe sobre el tratamiento de nuestra información personal, la Adjuntía en Asuntos Constitucionales de la Defensoría del Pueblo ha desarrollado este "Manual de protección de datos personales" con el objetivo de que la ciudadanía pueda conocer en forma clara, sencilla y didáctica qué son estos datos, cuál es el tratamiento que se les puede dar, cuáles son sus derechos frente a los bancos de datos, qué instrumentos tiene para defenderlos, así como la entidad encargada de protegerlos.

La recopilación y tratamiento permanente de esta información por parte de entidades públicas y privadas, requiere de mecanismos que permitan protegerlos adecuadamente y garanticen la posibilidad de efectuar un control sobre ellos, con la finalidad de evitar que un tratamiento indebido afecte directamente la intimidad personal y/o familiar, o sea utilizado para cometer actos ilícitos.

Actualmente, la Constitución Política reconoce el derecho fundamental a la autodeterminación informativa como una de las facultades que tienen las personas para resguardar su propia información ante el registro, uso y revelación de los datos que considere sensibles y que no deberían ser difundidos. A partir de ahí, el legislador ha establecido un marco legal para desarrollar este derecho a través de la Ley de Protección de Datos Personales – Ley 29733; y de su reglamento, aprobado por Decreto Supremo 003-2013-JUS.

Adjuntía en Asuntos Constitucionales
Defensoría del Pueblo

1. ¿Qué son los datos personales?

Son toda aquella información o dato que permite identificar a una persona natural o la hace identificable. Son datos personales:

- Nombre
- Imagen
- Voz
- Documento nacional de identidad
- Pasaporte
- Firma
- Domicilio
- Correo electrónico
- Huella dactilar, entre otros.

Cuando la información está estrechamente vinculada con la intimidad de la persona, los datos personales serán datos sensibles. Son datos sensibles:

- Datos biométricos
- Origen racial y étnico
- Ingresos económicos
- Opiniones o convicciones políticas
- Religión
- Afiliación sindical
- Toda información relacionada con la salud, o la orientación sexual.

¿Sabías que...?

El número de teléfono celular constituye un dato personal aun cuando no esté vinculado al nombre de una determinada persona, pues si bien no la identifica sí la hace identificable.

Toma nota:

Cuando se requiera el acceso a datos personales de funcionarios públicos, será necesario que se pondere el derecho a su intimidad frente al interés público de la ciudadanía.

¡Información importante!

- La imagen y la voz de una persona constituyen datos personales. Por ello, la difusión de información captada por una cámara de video vigilancia pública o privada está sujeta a los límites impuestos por la Ley de Acceso a la Información Pública, la Ley de Protección de Datos Personales y el Decreto Legislativo N° 1128.
- Las imágenes de un servidor público en el ejercicio de sus funciones serán públicas y de entrega vía procedimiento de acceso a la información siempre que se protejan los datos personales (voz e imagen) de personas ajenas a la función pública.

2. ¿Por qué proteger los datos personales?

La protección de datos personales es un derecho fundamental que le permite a toda persona preservar su intimidad y la de su familia frente a cualquier tratamiento desproporcionado, abusivo o irregular de sus datos personales.

En la actualidad, diversas actividades coidianas (asistir a una feria inmobiliaria, descargar unas aplicación web, participar en una red social, realizar compras por web, solicitar un crédito bancario, entre otras) implican la entrega de datos personales, por lo que resulta necesario darles un mínimo de protección.

La Constitución Política cautela los datos personales a través del derecho fundamental a la autodeterminación informativa, regulado en inciso 6 del artículo 2.

> **¿Sabías que...?**
>
> El derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de preservar su vida privada frente a posibles abusos o riesgos derivados de la utilización de sus datos.

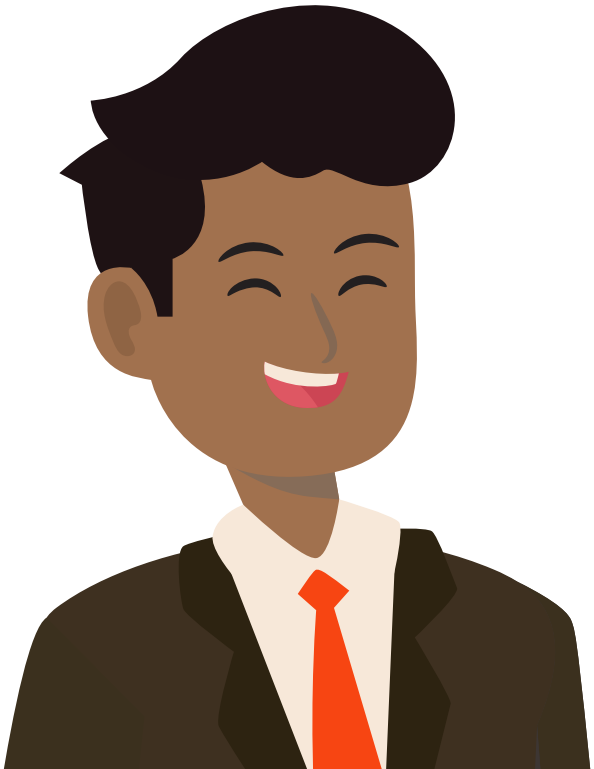
3. ¿Qué normas protegen los datos personales en el Perú?

A nivel nacional, los datos personales se encuentran protegidos por las siguientes normas:

1.- **Constitución Política del Perú**, prevé que los servicios informáticos, computarizados o no, públicos o privados, no suministren información que afecte la intimidad personal y familiar de las personas.

2.- **Ley 29733**, Ley de Protección de Datos Personales: desarrolla los derechos de los titulares de datos personales, los principios y las condiciones que se deben aplicar en su tratamiento.

3.- **Decreto Supremo 003-2013-JUS**, Reglamento de la Ley de Protección de Datos Personales: regula la inscripción en el Registro Nacional de Protección de Datos Personales así como el régimen sancionador ante la inobservancia de la normatividad sobre protección de datos personales.



> **Toma nota:**
>
> La Declaración Universal de Derechos Humanos y la Convención Americana de Derechos Humanos protegen los datos personales a través del derecho a la intimidad personal y familiar, y proscriben cualquier injerencia arbitraria en la vida privada.

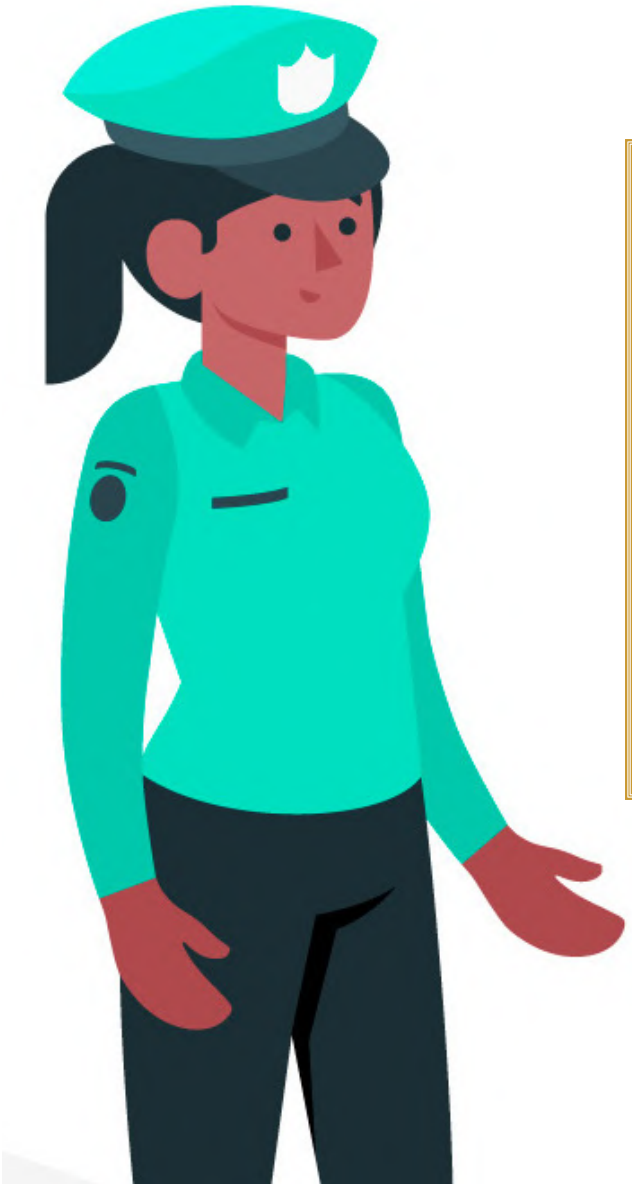
> **Dato útil**
>
> La Red Iberoamericana de Protección de Datos es un foro integrador de diversos actores públicos y privados, que promueve una regulación avanzada del derecho a la protección de datos personales.

4. ¿Cómo proteger los datos personales?

JUDICIALMENTE

A través del proceso de habeas data, el titular de los datos puede conocer, actualizar, incluir, suprimir o rectificar la información referida a su persona que se encuentre almacenada o registrada en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o privadas que brinden servicios o acceso a terceros. Asimismo, puede suprimir o impedir que se suministren datos de carácter sensible que afecten su intimidad.

Este proceso constitucional está reconocido en el artículo 200.3 de la Constitución Política y es desarrollado por el Código Procesal Constitucional.



ADMINISTRATIVAMENTE

A través de una solicitud dirigida al titular del banco de datos o al encargado del tratamiento, el titular del dato personal puede requerir el acceso, rectificación, corrección u oposición a cualquier tratamiento.

Si el titular del banco o el encargado se niegan o no responden la solicitud, entonces se puede iniciar un procedimiento trilateral de tutela ante la Autoridad Nacional de Protección de Datos Personales. La resolución que emita la Autoridad agota la vía administrativa, por lo que podrá ser cuestionada judicialmente vía proceso contencioso administrativo.

5. ¿Cuáles son los principios que guían el uso de datos personales?

Estos principios buscan brindar un nivel suficiente de protección a la información personal, por lo que deben ser aplicados por toda persona natural o jurídica que recopile y trate datos personales.

También son criterios interpretativos para aplicar la Ley 29733, Ley de Protección de Datos Personales, y su reglamento, así como para evitar vacíos en la aplicación de la legislación.

PRINCIPIOS PARA EL USO DE DATOS PERSONALES

Legalidad:

El tratamiento de datos personales debe realizarse conforme a los requisitos y disposiciones establecidas en la ley.

Consentimiento:

Se requiere autorización del titular para realizar el tratamiento de sus datos personales.

Finalidad:

Los datos personales deben ser recopilados y tratados solo para una finalidad determinada y lícita.

Proporcionalidad:

El tratamiento de datos personales debe ser conforme a su finalidad, evitando cualquier exceso.

Calidad:

Los datos personales que vayan a ser tratados deben ser veraces, exactos y actualizados.

Disposición de recurso:

Deben existir vías administrativas y jurisdiccionales para que los titulares de los datos personales puedan reclamar frente a algún tratamiento irregular.

Nivel de protección adecuado:

En el flujo transfronterizo de datos personales se debe garantizar un mínimo nivel de protección.

Seguridad:

El titular del banco de datos personales y el encargado del tratamiento deben brindar seguridad y protección a los datos que administran y tratan.

6. ¿En qué consiste el tratamiento de datos personales?

Es cualquier operación o proceso, automatizado o manual, que se realiza sobre los datos personales, tales como recopilación, grabación, registro, almacenamiento, conservación, uso, consulta, transferencia, modificación, supresión, bloqueo, entre otros.

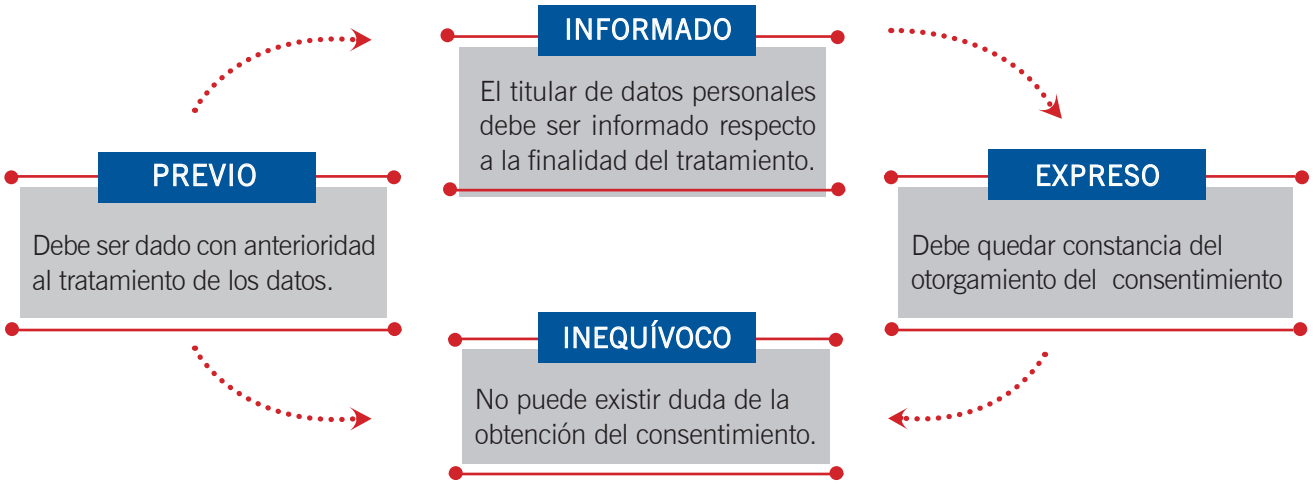
> **¿Sabías que...?**
>
> El límite para el tratamiento de datos personales es la autorización del titular del dato; es decir, la recopilación y transferencia de datos sin consentimiento es ilegal.

7. ¿Qué es el consentimiento para el tratamiento de datos personales?

El consentimiento para el tratamiento de datos personales es la autorización que debe brindar el titular para que sus datos puedan ser recopilados y tratados según la finalidad previamente informada.

La autorización puede brindarse de forma verbal o escrita; no obstante, para el tratamiento de datos sensibles es indispensable el consentimiento escrito.

Un consentimiento válido debe ser:



> **¿Sabías que...?**
>
> Para el tratamiento de datos personales de niñas, niños y adolescentes se requiere que los titulares de la patria potestad o tutores brinden el consentimiento. Excepcionalmente, las y los adolescentes entre 14 y 18 años podrán dar su consentimiento para el tratamiento de sus datos personales.

> **Toma nota:**
>
> La carga de la prueba respecto del consentimiento previo, expreso, libre e informado, la tiene el titular del banco de datos o quien resulte responsable del tratamiento.

8. ¿Cuándo no se requiere consentimiento?

La Ley 29733, Ley de protección de datos personales, regula aquellos casos en los que no se requiere solicitar autorización al titular de los datos personales para su tratamiento. Las excepciones al consentimiento se dan cuando:

> **Toma nota:**
>
> No proporciones más datos personales que los estrictamente necesarios. Por ejemplo, para contratar un crédito hipotecario no te pueden requerir datos relacionados a tu religión o identidad sexual.

1

Los datos personales son recopilados por entidades públicas para el cumplimiento de sus funciones.

Ejemplo: La ONP recopila datos de sus aportantes para cumplir con el pago de una pensión de jubilación, conforme a ley.

2

Los datos personales se encuentran contenidos en fuentes accesibles al público.

Ejemplo: El portal de transparencia estándar de una entidad pública contiene datos (nombre y DNI) de las personas que mantienen reuniones de trabajo con diversos funcionarios.

3

Se hace tratamiento de datos personales relativos a la solvencia patrimonial o de crédito.

Ejemplo: Las entidades financieras tienen acceso a datos personales relativos a la solvencia patrimonial o de crédito de sus clientes, para analizar la prestación de sus servicios.

4

Los datos personales son necesarios para la preparación, celebración y ejecución de un contrato en el que el titular de los datos es parte.

Ejemplo: Para comprar un inmueble se firmará un contrato entre la constructora y el particular, el cual debe consignar los datos personales que permitan identificar plenamente al comprador.

5

Se hace tratamiento de datos personales de salud, en circunstancias de emergencia, para prevenir, diagnosticar y tratar al titular, en centros de salud y por profesionales de la salud, observando el secreto profesional.

Ejemplo: El médico que atiende a personas afectadas en un accidente debe acceder a información de su salud, sin autorización, a efectos de realizar los tratamientos necesarios para salvaguardar su vida.

6

Se hace tratamiento de datos de los miembros de entidades sin fines de lucro, cuya finalidad sea política, religiosa o sindical, siempre que se circunscriba a sus actividades y que no sean transferidos sin consentimiento.

Ejemplo: La recopilación de datos de trabajadores adscritos a un sindicato, que permita la realización de sus actividades propias.

7

Se hubiera aplicado un procedimiento de anonimización o disociación.

Ejemplo: La Autoridad Nacional de Protección de Datos Personales publica los informes y consultas que emite en el ejercicio de sus funciones, para lo cual tacha los nombres y domicilios de las personas que intervinieron en el procedimiento.

8

El tratamiento de datos personales resulta necesario para salvaguardar intereses propios del titular.

Ejemplo: Ante la desaparición de una persona, las autoridades policiales tratan y publican sus datos personales para facilitar su ubicación.

9

Los datos personales son tratados para prevenir el lavado de activos, financiamiento del terrorismo u otros delitos, por mandato legal.

Ejemplo: Investigaciones iniciadas por el Ministerio Público por la presunta comisión del delito de lavado de activos, sin requerir consentimiento del investigado/a.

10

Las empresas obligadas a informar a la Unidad de Inteligencia Financiera deben brindar información de sus clientes para prevenir el lavado de activos y financiamiento del terrorismo.

Ejemplo: Las empresas del sistema financiero y sistema de seguros, la bolsa de valores, las cooperativas de ahorro y crédito y otros sujetos obligados comparten información de sus clientes, con fines preventivos, según la Ley 27693.

11

El tratamiento de datos se realiza en virtud del derecho fundamental de libertad de información.

Ejemplo: Medios de comunicación publican noticias de interés, relacionadas a la coyuntura política o social brindando datos personales de personas involucradas en hechos noticiosos.

¿Sabías que...?

Las excepciones a la obligación de solicitar el consentimiento del titular del dato no eximen el cumplimiento de las demás obligaciones y principios.

Toma nota:

Cuidado con los datos personales que publicas en tus redes sociales, ten en cuenta que muchas aplicaciones y juegos en línea requieren tu consentimiento para el acceso y tratamiento de tus datos.

9. ¿En qué consiste el flujo transfronterizo de datos?

El flujo transfronterizo consiste en la transferencia de datos personales hacia un destinatario que se encuentra en un país distinto del país de envío, cualquiera sea el soporte en que se encuentren, los medios utilizados para su transferencia o el tratamiento que reciban.

De acuerdo con el principio de nivel de protección adecuado, para transferir datos personales al extranjero se debe garantizar un nivel suficiente de protección para el tratamiento que se vaya a aplicar, que por lo menos sea equivalente a lo previsto en la Ley 29733 o a los estándares internacionales en la materia.

Si el país destinatario no cuenta con niveles adecuados de protección, el emisor del flujo transfronterizo deberá garantizar que el tratamiento de los datos personales se efectuará con respeto de los derechos de sus titulares.

> **Dato útil:**
>
> El titular del banco de datos o responsable del tratamiento podrá solicitar la opinión de la Dirección de Protección de Datos Personales respecto a si el flujo transfronterizo que realizará cumple con lo dispuesto por el marco legal.

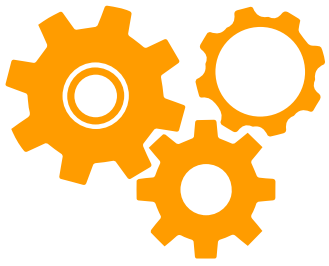
10. ¿Cómo brindar seguridad al tratamiento de datos personales?

El tratamiento constituye un procedimiento por el cual los datos personales son objeto de transferencia, conservación, difusión y otras actividades que impliquen su utilización, por lo que requieren indiscutiblemente la aplicación de medidas de seguridad. Para evitar la alteración, pérdida o acceso no autorizado a los datos, los titulares de bancos de datos personales deben aplicar las siguientes medidas de seguridad:

TÉCNICAS:

Medidas tecnológicas aplicadas a la información o al dato personal.

Ejemplo: Cifrar la información contenida en base de datos, generar copias de seguridad de los datos personales, entre otros.



ORGANIZATIVAS:

Políticas dispuestas para la protección y correcto tratamiento por el personal responsable y/o encargado de los bancos de datos.

Ejemplo: Identificar al personal autorizado para acceder a las bases de datos, conocer y clasificar los datos personales que posee la entidad, entre otros.

LEGALES:

Normas adecuadas para la protección de datos personales.

Ejemplo: Elaborar directivas internas que oriente el tratamiento de datos personales en la entidad, entre otros.

11. ¿Cómo proteger la confidencialidad en el tratamiento de datos personales?

La confidencialidad es el deber de guardar reserva respecto de los datos y sus antecedentes, que recae en el titular del banco de datos, en el encargado y en toda aquella persona que intervenga en el tratamiento.

El deber de confidencialidad concluye cuando medie consentimiento previo, informado, expreso e inequívoco del titular de los datos personales; ante una resolución judicial consentida o ejecutoriada; o cuando existan razones fundadas en la defensa nacional, seguridad pública o salud pública.

¿Sabías que...?

Un acceso no autorizado (ciberataque) que afecte la seguridad de los datos personales podría acarrear responsabilidad administrativa, si el encargado del tratamiento incumple las medidas de seguridad de la Ley de Protección de Datos Personales y su reglamento.

DERECHOS DEL TITULAR DE DATOS PERSONALES

12. ¿Qué son los derechos "ARCO"?

Son los derechos que tiene el titular de datos personales frente al titular del banco de datos o al encargado del tratamiento de sus datos.

Los derechos ARCO se ejercen personal y gratuitamente a través de solicitudes dirigidas al titular del banco de datos o al encargado del tratamiento. La solicitud de acceso deberá ser atendida dentro de los 20 días siguientes a su presentación, mientras que la de rectificación, cancelación y oposición, en el plazo de 10 días.

> **Dato útil:**
>
> El derecho al olvido es una vertiente del derecho a la protección de datos personales, que busca la supresión de datos contenidos en diversas fuentes de información. También es un mecanismo para preservar los derechos a la intimidad y al honor de las personas.

DERECHOS DEL TITULAR DE DATOS PERSONALES

- **Acceso:**

  Toda persona tiene derecho a conocer qué información sobre sí misma ha sido almacenada en un banco de datos público o privado; cómo y por qué fue recopilada; así como las transferencias realizadas o las que se prevén realizar.

- **Rectificación:**

  Toda persona tiene derecho a solicitar la modificación de los datos que fueron recopilados errónea, incompleta, inexacta, desactualizada o falsamente, en banco de datos público o privado. A su vez, permite la actualización e inclusión de nuevos datos personales.

- **Cancelación:**

  Toda persona puede requerir la cancelación o supresión de sus datos, cuando ya no cumplan una finalidad, cuando se haya revocado el consentimiento o haya transcurrido el plazo para su tratamiento.

- **Oposición:**

  Toda persona puede oponerse al tratamiento de sus datos personales almacenados en banco público o privado.

13. ¿Qué otros derechos tiene el titular de datos personales?

Además de los derechos ARCO, los titulares de datos personales tienen las siguientes facultades:

Derecho de información

El titular tiene derecho a ser informado respecto del tratamiento de sus datos, así como sobre la finalidad, los destinatarios, el banco en el que se almacenarán, el tiempo de conservación y lo relacionado con el tratamiento.

Derecho a impedir el suministro

Se podrá impedir que los datos personales sean suministrados a terceros, cuando estén en riesgo los derechos fundamentales del titular.

Derecho a la tutela

Si los derechos del titular de datos personales son negados total o parcialmente, el afectado podrá acudir a la Autoridad Nacional de Protección de Datos Personales o al Poder Judicial, a fin de ejercer la defensa de tales

Derecho a indemnización

En caso el titular de datos personales sea afectado como consecuencia del incumplimiento de la Ley de Protección de Datos Personales, tiene derecho a obtener la indemnización correspondiente.

14. ¿Qué son los bancos de datos?

El banco de datos personales es el conjunto organizado de datos de carácter personal, que se pueden encontrar en distintos soportes tales como físicos, magnéticos, digitales, ópticos, entre otros. Los bancos de datos pueden tener titularidad pública o privada, y pueden estar organizados de forma automática o manual.

Banco de datos de administración pública:

Los datos personales contenidos en estos bancos son administrados por una entidad pública.

Banco de datos de administración privada:

Los datos personales contenidos en estos bancos son administrados por una persona natural o jurídica de derecho privado, y no están vinculados al ejercicio de funciones públicas.

Se aplican las normas relativas a la protección de datos personales.

¡Información importante!

Los procedimientos de anonimización y disociación de datos personales impiden la identificación de su titular. Mientras que la anonimización es un procedimiento irreversible, la disociación sí puede revertirse. *(Ley de Protección de Datos Personales, artículos 2.14 y 2.15).*

15. ¿Quién es el titular y el encargado del tratamiento de datos personales?

El titular del banco de datos personales es aquella persona natural, persona jurídica privada o entidad pública que establece la finalidad para la recopilación y almacenamiento de los datos personales, así como el tratamiento y las medidas de seguridad que le serán aplicables.

Por su parte, el encargado del tratamiento de datos personales es aquella persona natural o jurídica, pública o privada, que realiza el tratamiento de los datos en nombre y por cuenta del titular del banco de datos. En caso realice un tratamiento ajena a la finalidad del encargo, podrá asumir responsabilidades.

16. ¿Qué obligaciones tiene el titular y el encargado del tratamiento de datos personales?

El titular del banco de datos y el encargado del tratamiento tienen las siguientes responsabilidades:

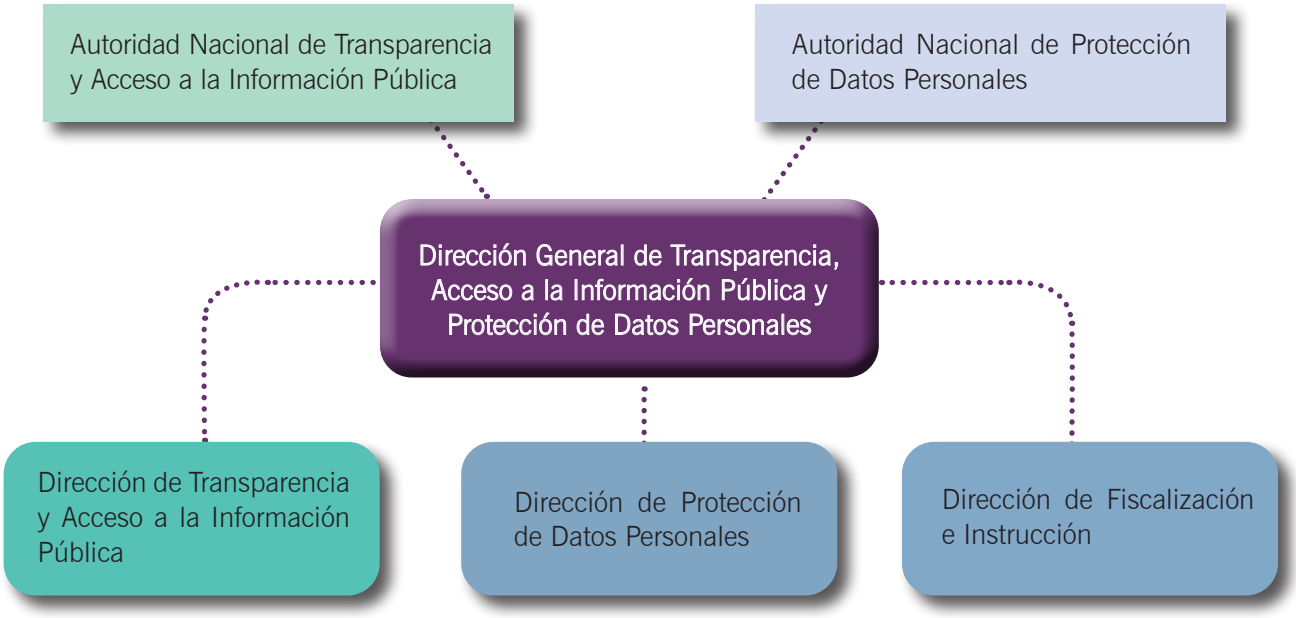
- Efectuar el tratamiento de datos personales solo si el titular ha dado un consentimiento válido.
- No recopilar datos personales de forma fraudulenta, desleal o ilícita.
- Recopilar solo aquellos datos que sean necesarios para alcanzar la finalidad previamente informada al titular.
- No utilizar los datos personales para finalidades distintas, salvo procedimiento de anonimización o disociación.
- No limitar el ejercicio de los derechos del titular de datos personales.
- Sustituir o complementar los datos personales cuando estos sean inexactos o incompletos.
- Eliminar aquellos datos personales que han dejado de ser necesarios o se haya vencido el plazo para su tratamiento.
- Proporcionar a la Autoridad Nacional de Protección de Datos Personales la información que requiera sobre el tratamiento de datos y el acceso a los bancos.

AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

17. ¿Qué es la Autoridad Nacional de Protección de Datos Personales?

La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales es el órgano que ejerce la Autoridad Nacional de Protección de Datos Personales, conjuntamente con la Autoridad Nacional de Transparencia y Acceso a la Información Pública.

La Autoridad Nacional de Protección de Datos Personales, que depende jerárquicamente del Despacho Viceministerial de Justicia del Ministerio de Justicia y Derechos Humanos, tiene como principal función garantizar el derecho fundamental de protección de datos personales.



18. ¿Cuáles son las funciones de la Autoridad Nacional de Protección de Datos Personales?

La Autoridad Nacional de Protección de Datos Personales tiene las siguientes funciones:

- Resolver en última instancia los procedimientos administrativos sancionadores impulsados por la Dirección de Fiscalización e Instrucción.
- Resolver las reclamaciones de los titulares de datos personales por denegación de sus derechos ARCO.

Imponer multas accesorias a las sanciones impuestas en el procedimiento sancionador.

Actualizar y supervisar el Registro Nacional de Protección de Datos Personales.

Inscribir y supervisar las comunicaciones de flujo transfronterizo de datos personales.

Emitir opinión técnica vinculante de los proyectos de ley sobre datos personales.

Absolver consultas sobre protección de datos personales y promover campañas de difusión y promoción del derecho.

Ejecutar las sanciones administrativas impuestas y hacer cumplir las medidas cautelares aplicadas.

Inscribir los bancos de datos personales de la administración pública o privada.

Cancelar la inscripción de bancos de datos personales públicos o privados, a solicitud de parte.

Certificar la existencia o no de inscripciones en el Registro Nacional de Protección de Datos Personales.

Emitir directivas sobre seguridad de banco de datos personales y supervisar su cumplimiento.

¿Sabías que...?

El personal que labora en la Autoridad Nacional de Protección de Datos Personales debe guardar confidencialidad en relación a los datos que conozca en ejercicio de sus funciones, bajo responsabilidad. *(Ley de Protección de Datos Personales, artículo 35).*

Toma nota:

En el Registro Nacional de Protección de Datos Personales se inscriben los bancos de datos de administración pública o privada a nivel nacional, los flujos transfronterizos de datos que se realicen, así como las sanciones impuestas. *(Ley de Protección de Datos Personales, artículo 34).*

19. ¿En qué consiste el procedimiento trilateral de tutela?

Para ejercer los derechos ARCO, el titular del dato personal debe presentar una solicitud ante el titular del banco de datos o el encargado del tratamiento, en la que requiere el acceso, la rectificación o la cancelación de sus datos, o indique la oposición a su tratamiento. Si el titular o el encargado emiten una respuesta insatisfactoria, deniegan la solicitud o no la responden en los plazos establecidos, se debe presentar una solicitud de tutela de derechos, ante la Autoridad Nacional de Datos Personales. Tras solicitar los descargos del reclamado, la Dirección de Protección de Datos Personales resuelve en primera instancia los procedimientos trilaterales de tutela, puede imponer sanciones administrativas (multas).

Finalmente, la decisión puede ser recurrida en apelación ante la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Esta resolución agota la vía administrativa.

El procedimiento trilateral tiene las siguientes etapas:

Solicitud de derechos ARCO

Ante el titular del banco de datos o encargado del tratamiento.

Solicitud de tutela de derechos

Ante la Dirección de Protección de Datos Personales.

Recurso de apelación

Ante la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Resolución Directoral N° 035-2015-JUS/DGPDP

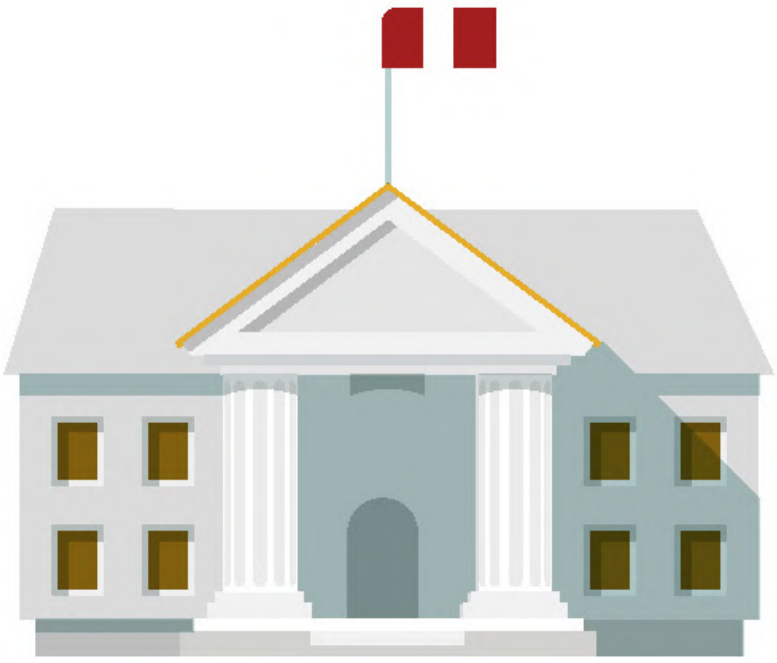
En el 2015, la Dirección General de Protección de Datos Personales sancionó al administrador de un blog con una multa de 1 UIT, por haber realizado un tratamiento de los datos personales (imagen y DNI) de los gerentes de una determinada persona jurídica, sin contar con su consentimiento. La Dirección ordenó bloquear y suprimir los referidos datos personales y adoptar medidas para realizar un tratamiento en concordancia con las normas legales.

Resolución Directoral N° 453-2018-JUS/DGTAIPD-DPDP

La Dirección de Protección de Datos Personales sancionó a un medio de comunicación por no haber dado respuesta al pedido de supresión de datos del reclamante, respecto de una noticia en la que aparecía como testaferro de una organización criminal, con información errónea. La Dirección ordenó actualizar la noticia e indexarla junto al título de la noticia que hacía alusión a la calidad de testaferro del ciudadano.

Resolución Directoral N° 747-2018-JUS/DGTAIPD-DPDP

La Dirección de Protección de Datos Personales sancionó a una empresa de telecomunicaciones por negarse a eliminar los datos personales (número de celular, correo electrónico, dirección) del reclamante. La Dirección ordenó cancelar los datos registrados en su banco de datos denominado “Clientes – BI MDM”. La resolución fue confirmada por la Dirección General de Transparencia, Acceso a la Información y Protección de Datos Personales, mediante la Resolución Directoral N° 14-2019-JUS/DGPDP, del 25 de febrero de 2019.



20. ¿En qué consiste la facultad sancionadora de la autoridad?

La Autoridad Nacional de Protección de Datos Personales puede iniciar, de oficio o a petición de parte, un procedimiento administrativo sancionador contra el titular del banco de datos, de administración pública o privada, que incurra en cualquiera de las infracciones tipificadas en el Reglamento de la Ley de Protección de Datos Personales.

El procedimiento administrativo sancionador tiene las siguientes etapas:

Etapa de Instrucción

Dirección de Fiscalización e Instrucción

Plazo: 50 días hábiles

Resolución en primera instancia

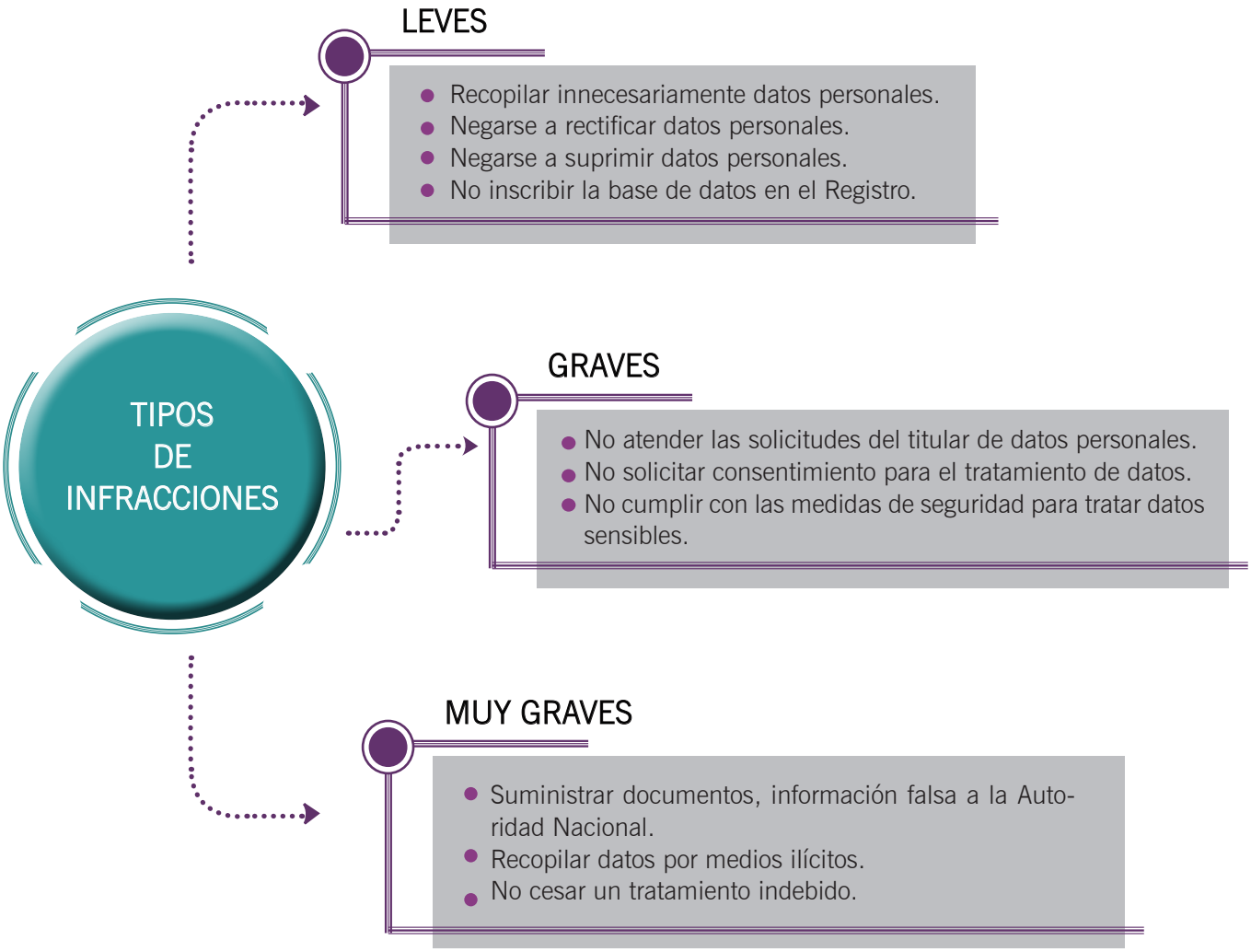
Dirección de Protección de Datos Personales

Plazo: 20 días hábiles

Resolución en segunda instancia

Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales

De haberse acreditado la responsabilidad por la comisión de alguna infracción, la Autoridad podrá imponer sanciones administrativas, medidas correctivas y multas coercitivas.



El monto de las multas dependerá de la gravedad de la infracción cometida, será determinada por unidades impositivas tributarias y para su aplicación se tomará en cuenta la subsanación realizada dentro del procedimiento sancionador.

Resolución Directoral N° 025-2016-JUS/DGPDP/DS

En el 2016, La Dirección de Sanciones impuso una multa de 2.5 UIT a un centro educativo por haber efectuado el tratamiento de imágenes de sus alumnos en su página web, sin el consentimiento de los padres de familia o tutores. Además, impuso la multa de 8 UIT por no haber inscrito el banco de datos de sus alumnos en el Registro Nacional de Protección de Datos Personales.

Resolución Directoral N° 158 -2016-JUS/DGPDP-DS

En el 2016, la Dirección de Sanciones impuso una multa de 8 UIT a una clínica privada por haber realizado un tratamiento desproporcionado de los datos personales referidos a la religión de los postulantes a un puesto de trabajo. La sanción fue confirmada por la Dirección General de Protección de Datos Personales, mediante la Resolución Directoral N° 065-2016-JUS/DGPDP, del 19 de agosto de 2016.

Resolución Directoral N° 04-2018-JUS/DGTAIPD

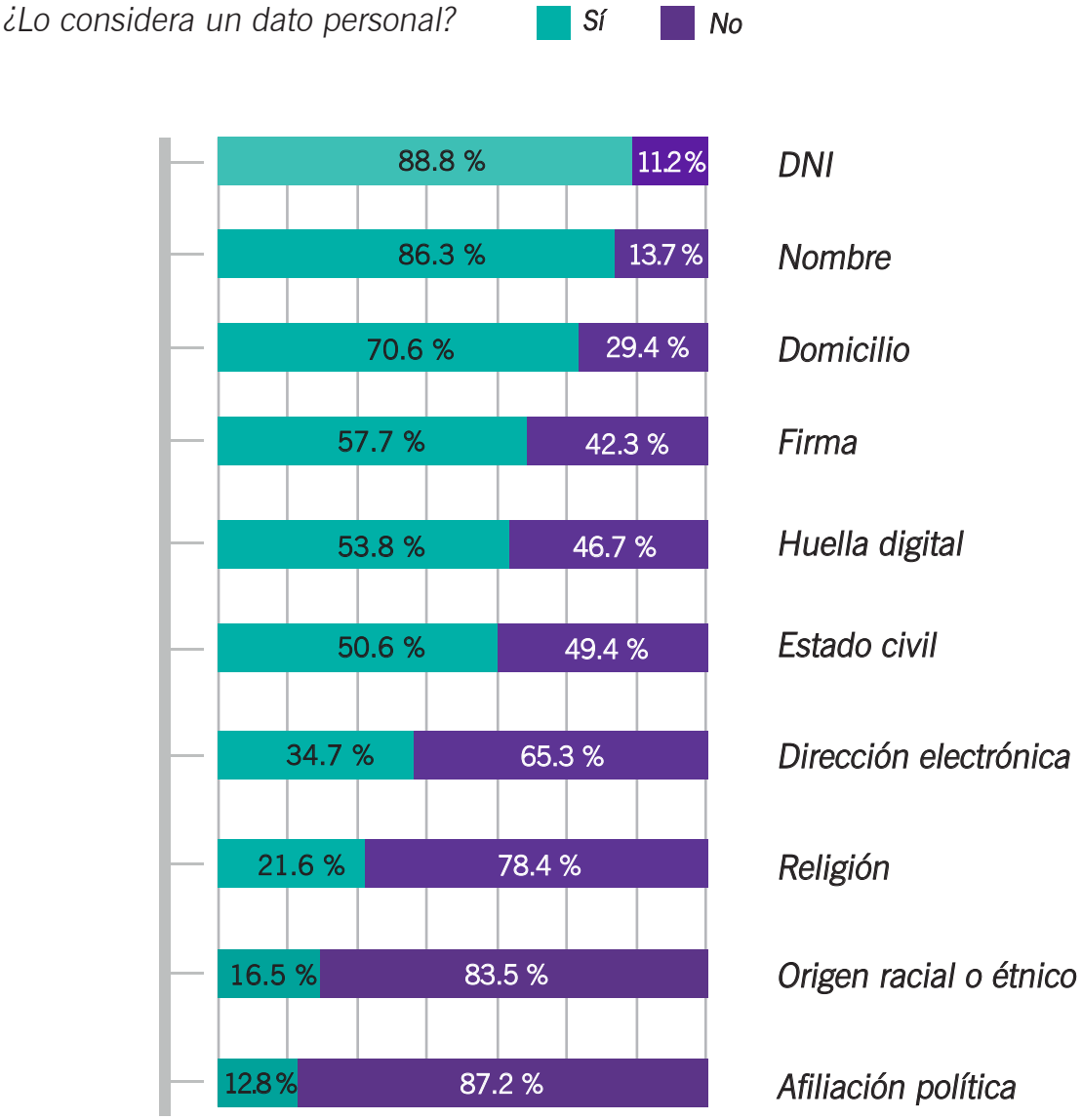
La Dirección Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales impuso una multa de 30.25 UIT a una agencia de viajes por haber solicitado a los postulantes datos sensibles vinculados con su salud (prueba de VIH) y evaluarlo en un proceso de selección de un puesto de trabajo, en contravención del principio de proporcionalidad. Además, impuso la multa de 1.31 UIT por realizar tratamiento de datos sensibles sin cumplir con las medidas de seguridad correspondientes.

SOBRE ESTA EDICIÓN

Con el objetivo de conocer el estado del derecho de protección de datos personales, la Adjuntía en Asuntos Constitucionales de la Defensoría del Pueblo requirió información a las oficinas defensoriales, módulos de atención defensorial y demás oficinas acerca de casos atendidos e interrogantes sobre el ámbito de protección de los datos personales.

Asimismo se solicitó a las oficinas defensoriales y módulos de atención su colaboración para aplicar, de forma voluntaria, encuestas a aquellas personas que acudan a las distintas sedes de la Defensoría del Pueblo entre julio y agosto de 2019, a fin de recoger información respecto de su conocimiento sobre la protección de sus datos personales.

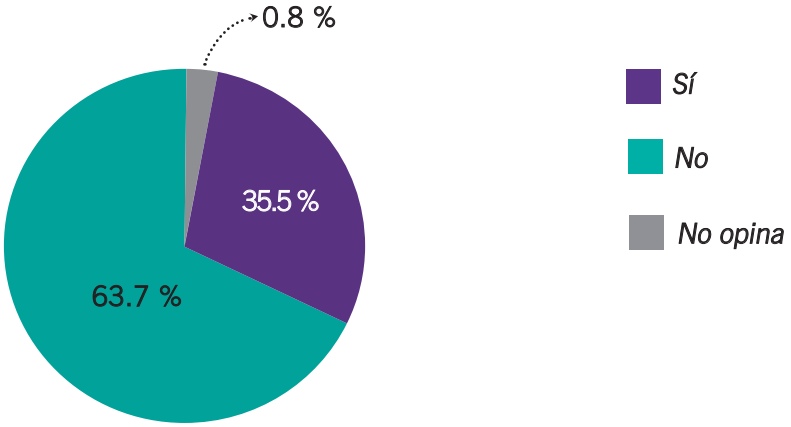
Se aplicaron un total de 626 encuestas, en 29 oficinas y 4 módulos de atención. Tras los resultados, se evidenció que un alto porcentaje de personas no reconoce la afiliación política, el origen racial o la religión como datos personales, a pesar de que son datos sensibles.



Elaboración: adjuntía en asuntos constitucionales

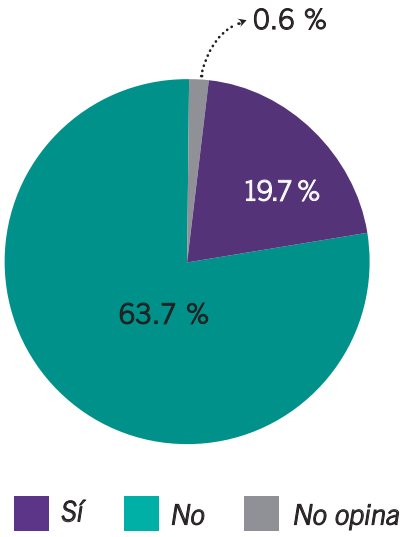
En la misma línea, la mayoría de las personas encuestadas desconocen la existencia de un dispositivo legal que proteja sus datos personales (63,7%); desconocen en qué consisten sus derechos de acceso, rectificación, cancelación y oposición (94,3%); y afirman no haber ejercido tales derechos (63,7%).

¿Conoce alguna ley que proteja sus datos personales?

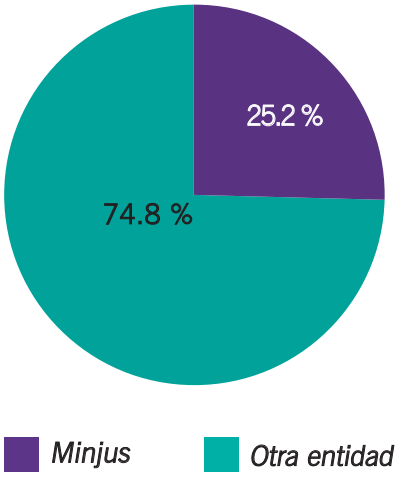


Finalmente, solo 123 (19,7%) personas encuestadas conocían de la existencia de alguna institución pública que se encargue de la protección de datos personales. De dicho porcentaje, solo 31 personas reconocieron al Ministerio de Justicia y Derechos Humanos como tal institución.

¿Conoce alguna institución pública que protega sus datos personales?



¿Cuál es esa institución?



Elaboración: adjuntía en asuntos constitucionales

En consideración a la situación descrita, la Adjuntía en Asuntos Constitucionales está convencida de que el presente manual servirá como guía para que la población conozca estos derechos en específico, así como los mecanismos e instituciones de protección.

ENCUESTA DEFENSORIAL SOBRE PROTECCIÓN DE DATOS PERSONALES

Finalidad: recoger información respecto del conocimiento que tiene la población sobre la protección que deben recibir sus datos personales. Dicha información será consolidada e incluida en el "Manual sobre protección y debido tratamiento de datos personales" que desarrollará la Defensoría del Pueblo.

Sírvase responder de forma anónima, las siguientes preguntas:

1. Edad: _____

2. ¿Cuál(es) son dato(s) personal(es)?

Nombre	☐	Origen racial o étnico	☐
Numero DNI	☐	Religión	☐
Domicilio	☐	Estado civil	☐
Afiliación política	☐	Huella digital	☐
Dirección electrónica	☐	Firma	☐

3. ¿Considera que la protección de sus datos personales constituye un derecho fundamental?

Sí ☐ No ☐

4. ¿Conoce de alguna ley que proteja sus datos personales?

Sí ☐ No ☐

5. Conoce en qué consisten los derechos "ARCO" (Acceso, rectificación, cancelación y oposición) aplicable a sus datos personales?

Sí ☐ No ☐

6. ¿Ha ejercido algún derecho "ARCO" frente a una entidad pública o empresa privada?

Sí ☐ No ☐

7. ¿Alguna empresa le ha pedido consentimiento para el uso de sus datos personales? (ejemplo: bancos, empresas de telefonía, seguros)

Sí ☐ No ☐

8. ¿Sabe cuál es la institución pública que fiscaliza el cumplimiento de las normas en protección de datos personales?

Sí ☐ No ☐ ¿Cuál? .....

REFERENCIAS

- Tribunal Constitucional del Perú

  - Expediente 00300-2010-HD/TC

- Tribunal de Transparencia y Acceso a la Información Pública

  - Expediente 00178-2019-JUS/TTAIP

- Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales

  - Informe 27-2017-JUS/DGTAIPD-DPDP
  - Opinión Consultiva 007-2019-JUS/DGTAIPD
  - Opinión Consultiva 019-2019-JUS/DGTAIPD
  - Opinión Consultiva 026-2019-JUS/DGTAIPD
  - Opinión Consultiva 037-2019-JUS/DGTAIPD

- Dirección de Fiscalización e Instrucción de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales

  - Informe 013-2018-DFI-VARS

- Tribunal Constitucional de España

  - Sentencia 58/2018

Defensoría
del Pueblo