

GUÍA PARA CUMPLIR LA NORMATIVA SOBRE PROTECCION DE DATOS PERSONALES **‘PROTEGIENDO LOS DATOS PERSONALES, PROTEGEMOS A LOS CIUDADANOS EN EL SECTOR PÚBLICO’**



PROTEGIENDO LOS DATOS PERSONALES PROTEGEMOS A LOS CIUDADANOS

Abreviaturas	3
Introducción	4
1. ¿Qué se protege con la Ley sobre Protección de Datos Personales?	6
2. ¿Quién está obligado a proteger los datos personales?	7
3. ¿Cuándo manejamos datos personales?	8
4. ¿Cuándo comienza la protección de los datos personales?	9
5. ¿Qué obligaciones implica el tratamiento de datos personales?	10
a. Elaborar la Ficha técnica	10
b. Cumplir con los principios generales en protección de datos personales	12
c. Condiciones de licitud para el tratamiento de los datos personales	14
d. Elaborar el registro de las bases de datos	16
e. Garantizar la seguridad de los datos personales	17
f. Realizar transferencias de datos a terceros con garantías	18
g. Designar un Oficial de Protección de Datos	20
h. Atender y dar respuesta al ejercicio de los derechos de los titulares de los datos personales	20
6. ¿Quién es la Autoridad encargada de velar por el cumplimiento de esta normativa?	22
7. ¿Cómo actuar ante una denuncia por incumplir la Ley 81 de 2019?	23
Hoja de ruta para el cumplimiento:	¡Error! Marcador no definido.

Abreviaturas

En esta Guía se utilizarán las siguientes siglas:

- * ANTAI: Autoridad Nacional de Transparencia y Acceso a la Información.
- * AIG: Autoridad Nacional para la Innovación Gubernamental.
- * Ley 81 de 2019: Ley No. 81 de 26 de abril de 2019 sobre Protección de Datos Personales publicada en Gaceta Oficial el 29 de marzo de 2019.
- * Decreto Ejecutivo 285 de 2021: Decreto Ejecutivo No. 285 de 28 de mayo de 2021 Que reglamenta la Ley 81 de 2019 sobre Protección de Datos personales publicado en Gaceta Oficial el 28 de mayo de 2021.

Introducción

El desarrollo de la Administración electrónica y el avance de las nuevas tecnologías tienen un impacto en la privacidad de los ciudadanos que debemos medir y balancear. En esta guía queremos ayudar a las entidades públicas a conocer el valor que aportan a la sociedad al cumplir con la normativa sobre protección de datos personales. A través de la protección de la información personal que manejamos en el día a día, las entidades públicas protegemos mejor a los ciudadanos cuando protegemos sus datos personales en los tratamientos que realizamos sobre ellos en el día a día.

De este modo y para contribuir con las entidades públicas a tomar conciencia de la necesidad de garantizar la protección de los datos personales a los ciudadanos, haremos un recorrido por la normativa, para conocer el impacto que tiene en las actividades y servicios públicos. Explicaremos cuáles son las obligaciones que las entidades públicas deben cumplir como sujetos obligados y los derechos que debemos garantizar a los ciudadanos en el tratamiento de sus datos personales.

En esta guía daremos pautas generales de cumplimiento que sirvan para todas, sin perjuicio de que atendiendo a las funciones de servicio público que cada entidad deba desarrollar, se deban tener en cuenta, además, otras pautas de cumplimiento.

El derecho a la protección de datos personales ha sido reconocido en el artículo 42 de nuestra Constitución Política, así como en innumerables textos internacionales como el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, conocido como Convenio 108 del Consejo de Europa¹ y en cuya memoria celebramos el Día Internacional de la Protección de Datos Personales el 28 de enero de cada año. Las Directrices de Privacidad de la Organización para la Cooperación y el Desarrollo Económicos, OCDE², los Principios actualizados sobre la Privacidad y la Protección de Datos Personales de la Organización de los Estados Americanos, OEA³, el Reglamento Europeo de Protección de Datos o los Estándares de Protección de Datos Personales para los Estados Iberoamericanos de la Red Iberoamericana de Protección de Datos⁴, RIPD, entre otros.

¹ Puedes consultar el texto aquí: <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>

² Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, conocidas como “directrices de privacidad”, fueron adoptadas, el 23 de septiembre de 1980, como una recomendación del Consejo de la OCDE apoyando los tres principios que aglutinan a los países de la OCDE: democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas.

Se pueden consultar las Directrices aquí:

<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>

³ Aprobados en 2012 y actualizados en 2021 pueden consultarse aquí: https://www.oas.org/es/sla/ddi/proteccion_datos_personales_Principios_CJI_2012.asp (Fecha de consulta 11 de abril de 2023)

⁴ Pueden consultarse aquí: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf (Fecha de consulta: 11 de abril de 2023).

En la República de Panamá, este derecho de los ciudadanos está regulado en la Ley 81 de 26 de abril de 2019 sobre Protección de Datos Personales. Esta Ley constituye el marco general de protección de datos en la República y está desarrollada reglamentariamente por el Decreto Ejecutivo 285 de 28 de mayo de 2021. Complementa así el mandato constitucional, establecido en el artículo 42 de la Constitución Política, de proteger la privacidad de las personas y las leyes especiales que se han aprobado en la República de Panamá antes de la Ley 81 de 2019 y las leyes especiales que lo hagan después de la misma.

La Ley 81 de 2019 se refiere al tratamiento de datos personales, por parte de entidades públicas, entre otros, en su artículo 29, donde dispone que estarán legitimadas para efectuar los tratamientos de datos personales respecto de las materias de su competencia y con sujeción a lo establecido en la Ley. Esto es, las entidades públicas deben cumplir los mandatos de la Ley 81 de 2019 en todos los tratamientos de datos personales que realizan en el desarrollo de las competencias públicas que tienen atribuidas en la República de Panamá.

Comenzamos...

1. ¿Qué se protege con la Ley sobre Protección de Datos Personales?

La Ley sobre Protección de Datos Personales de la República de Panamá, define los datos personales como:

“cualquier información concerniente a personas naturales, que las identifica o las hace identificables”.

Esto es, el objeto de protección son los **datos personales de las personas naturales** cuando son **objeto de tratamiento**. La Ley define tratamiento como:

“cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permita recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, asociar, disociar, comunicar, ceder, intercambiar, transferir, transmitir o cancelar datos, o utilizarlos en cualquier otra forma.”

Los datos personales pueden ser de naturaleza muy diversa, por ejemplo, podemos hablar de **datos identificativos** de la persona, esto es, los que la identifican directamente, como son: nombre y apellido; y podemos hablar de **datos que hacen identificable** a una persona natural, como son: número de cédula de identidad; número de celular; dirección postal; correo electrónico; ...

También son datos personales otros datos que la ley define como **datos sensibles**, por la información personal que revelan de cada uno y por la posibilidad de que su uso indebido conlleve situaciones de discriminación: datos de salud, datos sobre origen racial o étnico, opiniones políticas, orientación sexual, creencias religiosas, datos biométricos como la huella digital o el reconocimiento facial y datos genéticos.

Dato que identifica	Dato identificable	Dato sensible
<ul style="list-style-type: none"> • Nombre y apellidos • Fotografía 	<ul style="list-style-type: none"> • Número de cédula de identidad • Número de cita • Número de cliente • Número de paciente 	<ul style="list-style-type: none"> • Salud • Origen racial • Opinión política o religiosa • Vida u orientación sexual • Datos genéticos • Datos biométricos: huella digital

2. ¿Quién está obligado a proteger los datos personales?

La Ley 81 de 2019 distingue varios roles que están llamados a cumplir sus exigencias. Los roles que pueden tener los sujetos obligados son responsable del tratamiento o custodio de la base de datos.

- * **Responsable del tratamiento:** es la entidad pública, en el caso de la guía que nos ocupa, que es titular de la base de datos en la que los datos personales van a ser tratados. Para conseguir sus fines decide qué datos y cuál es el alcance del tratamiento que quiera realizar, así como de los medios que dispone para ello.

Las entidades públicas son responsables del tratamiento de las bases de datos que manejan en el desarrollo de su actividad pública. Por ejemplo:

- * base de datos de recursos humanos: incorpora los datos personales de los funcionarios públicos y aglutina todos los tratamientos de datos que se realizan de los funcionarios públicos o, en su caso, empleados, que prestan servicio en la entidad pública;
- * base de datos de usuarios de servicios públicos: formada por los datos personales de los ciudadanos usuarios de los servicios públicos y se refiere a todos los tratamientos de datos de los ciudadanos que deriven de la prestación de los servicios públicos;
- * base de datos de proveedores: incorporan los datos personales y los tratamientos de datos que derivan de las relaciones comerciales con los proveedores de productos o servicios;
- * bases de datos de relaciones públicas: formada por los datos de contacto de la agenda de relaciones públicas e institucionales de la entidad;
- * etc.

Al responsable del tratamiento le corresponde tomar las decisiones relacionadas con el tratamiento de los datos. Esto es, qué datos necesita recopilar y con qué finalidad para cumplir con las exigencias legales que derivan de las relaciones con los funcionarios de carrera administrativa, de los usuarios de servicios públicos, etc.

- * **Custodio de la base de datos:** este rol lo ocupa la empresa o ente público que, para prestar un servicio al responsable del tratamiento, accede a los datos personales que forman parte de su base de datos por cuenta suya y bajo su mandato.

Las entidades públicas también pueden actuar como encargados del tratamiento respecto de las bases de datos de terceros. Pensemos en la entidad pública que desarrolla y da mantenimiento a plataformas de servicios públicos como las de la Dirección General de Ingresos (DGI), la Caja del Seguro Social (CSS), la de denuncias a través de la plataforma SmartCID, etc.

3. ¿Cuándo manejamos datos personales?

Una de las primeras tareas que las entidades públicas deben llevar a cabo es la de identificar los tratamientos de datos personales que realizan, así como definir los colectivos a los que corresponden estos datos personales, de un lado, y analizar la finalidad o finalidades de tratamiento, así como la condición de licitud del tratamiento, de otro lado.

Las entidades públicas manejan datos personales en el desarrollo de sus funciones públicas. Y manejan datos de distintos **colectivos** respecto de los que deben observar las exigencias de la normativa sobre protección de datos personales.

Así, tratan datos de los **ciudadanos**, por ejemplo:

- * al tomar cita a los ciudadanos para la gestión de algún servicio público;
- * al registrar a los ciudadanos en los registros públicos;
- * en el registro de entrada y salida de las oficinas o sedes;
- * al atender el teléfono de atención ciudadana;
- * en los formularios de toma de datos de sus portales de internet;
- * en los formularios en papel que deben completar los ciudadanos, etc.

También tratan datos personales de los **funcionarios públicos** designados en sus servicios e instituciones. Así, por ejemplo, en el área de recursos humanos tienen los expedientes de los funcionarios asignados, de los solicitantes de empleo, pueden llevar un registro horario de los funcionarios, control de vacaciones y días libres, en definitiva, realizan muchos tratamientos de datos de cada uno de los colectivos de los que tratan datos personales.

Otro colectivo del que manejan datos es de los **proveedores** de productos y servicios, así, manejan sus datos en los contratos con proveedores, en las solicitudes de pedido, en las facturas, en la contabilidad que llevan en la entidad.

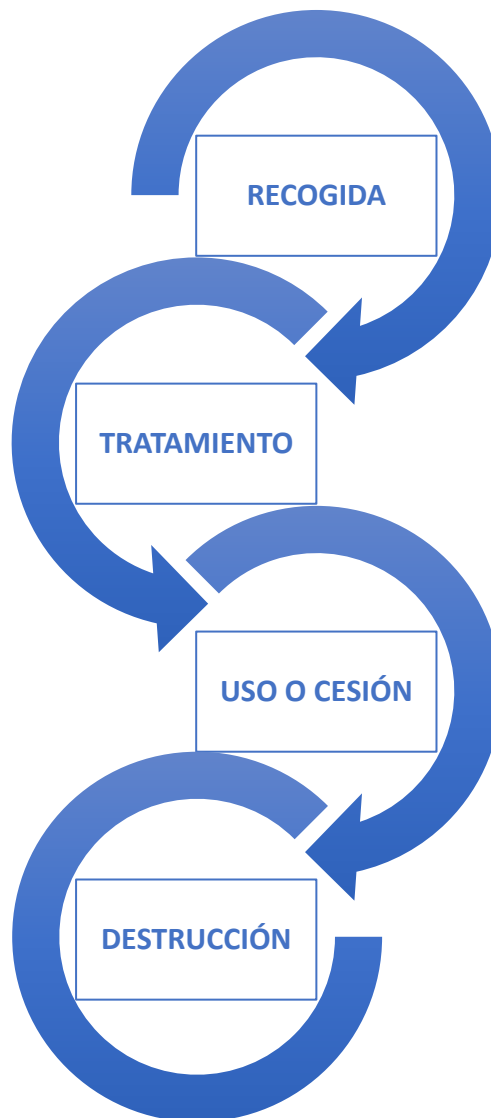
Además, el manejo de los datos personales puede tener lugar a través de distintos **canales**:

- * Presencialmente;
- * telefónicamente;
- * a través de plataformas de internet, para prestar servicios de administración electrónica,
- * a través de distintos dispositivos de toma de datos: cámaras de videovigilancia, sistemas de control de entrada y salida de personas de nuestras instalaciones a través de registro por huella dactilar o reconocimiento facial;
- * a través de terceros a los que contratan servicios que impliquen toma de datos: empresas de desarrollo y mantenimiento de software, empresas que organicen eventos, capacitaciones, actos académicos, etc., para la entidad;

- * a través de contratos: por ejemplo, con proveedores o personal designado a la entidad.

4. ¿Cuándo comienza la protección de los datos personales?

La protección de datos personales comienza con la toma de datos y termina con la destrucción de estos. Durante este tiempo, hay momentos claves para su protección, es lo que conocemos como el **ciclo de vida del dato**:



Durante todo el ciclo de vida del dato personal bajo nuestra responsabilidad, debemos observar todas las exigencias que derivan de la normativa sobre protección de datos personales.

5. ¿Qué obligaciones implica el tratamiento de datos personales?

Para las entidades públicas es fundamental comprender su función en relación con los datos personales que están manejando en el cumplimiento de las funciones públicas que tienen encomendadas. De esta forma, podrán garantizar el cumplimiento de la normativa y lo que es más importante proteger a los ciudadanos en el tratamiento de sus datos personales.

En este sentido, lo recomendable es que se tomen un tiempo para analizar los tratamientos de datos que llevan a cabo en su actividad pública y poder así elaborar la denominada en la Ley “Ficha técnica” que comprende los protocolos, procesos y procedimientos de gestión y transferencia segura de los datos personales de los que son responsables del tratamiento.

Veamos las **principales obligaciones** que deben ser cumplidas por los sujetos obligados. Estas obligaciones se pueden resumir en los siguientes grupos:

- 1) Elaborar la Ficha técnica compuesta por los protocolos, procesos y registros de cumplimiento.
- 2) Cumplir los principios generales que rigen la protección de datos.
- 3) Basar el tratamiento de los datos personales en una de las condiciones de licitud previstas en la normativa.
- 4) Garantizar la seguridad de los datos personales mediante la adopción de medidas técnicas y organizativas.
- 5) Adoptar garantías en las transferencias de datos personales a terceros.
- 6) Atender y dar respuesta al ejercicio de los derechos de los titulares de los datos.
- 7) Designar un Oficial de Protección de Datos (OPD).

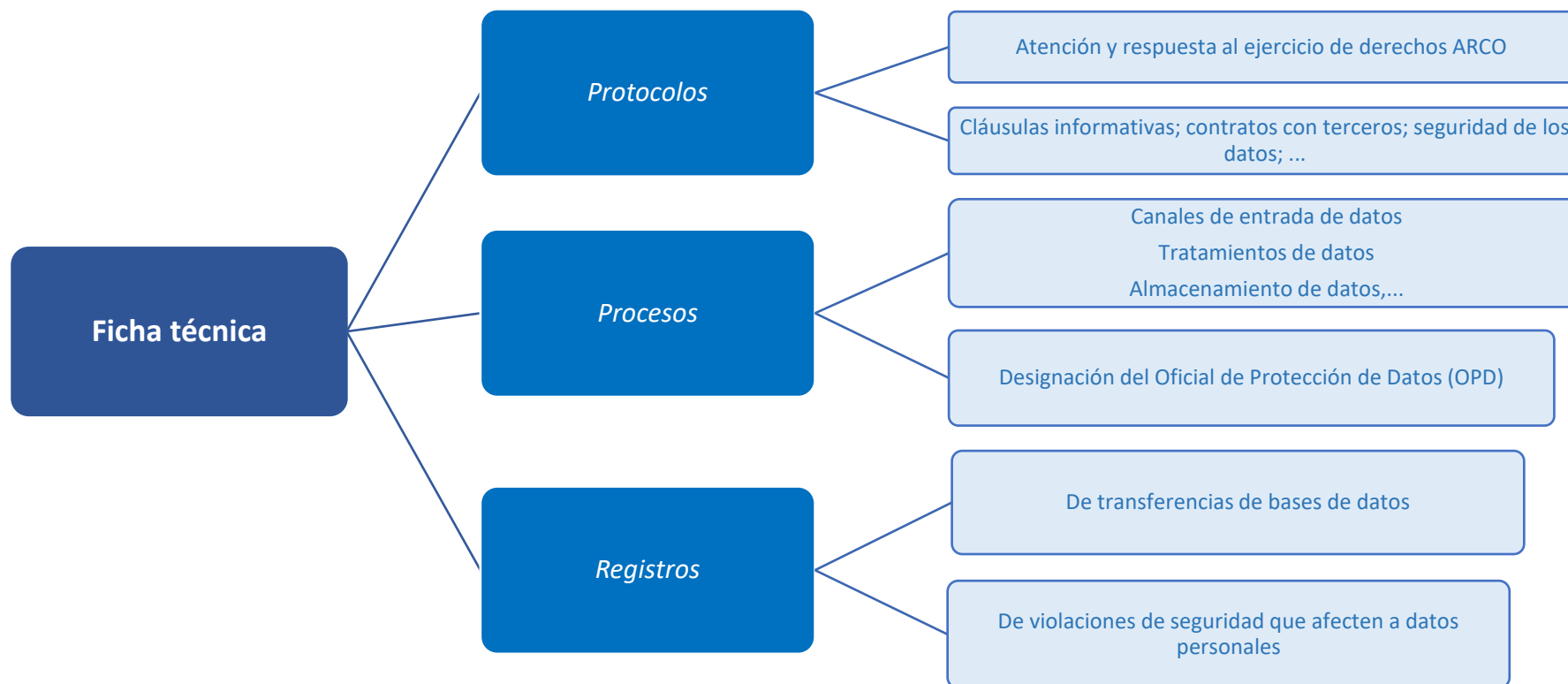
a. Elaborar la Ficha técnica

La Ley 81 de 2019 define la Ficha Técnica como:

“Documento que contiene los registros, protocolos y reglas, relacionados al almacenamiento y tratamiento de los datos personales”

De este modo, la Ley traslada al responsable o custodio de la base de datos la obligación de elaborar los registros, protocolos y reglas o procedimientos de gestión y transferencia segura de los datos personales que sean necesarios en el desarrollo de su actividad pública ligada al tratamiento de los datos personales.

En el gráfico siguiente se recoge lo que podría ser un ejemplo del contenido principal de esta Ficha Técnica:



b. Cumplir con los principios generales en protección de datos personales

La Ley 81 de 2019 establece unos **principios generales** que podemos considerar los principios que deben regir nuestra actuación en relación con el tratamiento de los datos personales.

Lealtad tratar datos sin engaño o fraude	Finalidad tratar datos con fines determinados y plazo de conservación	Proporcionalidad tratar datos adecuados, pertinentes y mínimo necesario
Veracidad y exactitud realizar tareas de actualización de datos	Seguridad de los datos adoptar medidas técnicas y organizativas	Transparencia lenguaje sencillo y claro
Confidencialidad compromiso respecto de los datos personales	Licitud obligación legal, consentimiento, relación contractual,...	Portabilidad derecho de los titulares

- * **Principio de lealtad:** este principio exige que los datos sean recolectados para un tratamiento sin utilizar engaño, ni medios fraudulentos, desleales o ilícitos;

El ciudadano debe ser consciente en todo momento de que estamos tratando su información personal.

- * **Principio de finalidad:** este principio exige, de un lado, que el tratamiento de los datos personales responda a una finalidad determinada y legítima.

Para delimitar el tratamiento a unos fines determinados y legítimos, la entidad pública como el responsable del tratamiento debe detenerse a pensar y definir cuáles son estos fines.

Por otro lado, exige también que los datos no sean tratados con fines incompatibles o diferentes a los que motivaron la recogida de los datos.

El uso de los datos con fines distintos implica la necesidad de analizar qué condición de licitud legitima ese nuevo tratamiento y qué pasos se deben dar en la dirección de realizar un tratamiento legal de esos datos.

Una tercera y última exigencia es la de delimitar el plazo de conservación de los datos.

Podemos conservar los datos durante el tiempo necesario para cumplir la finalidad del tratamiento y, además, por el plazo durante el que se pueden ejercitar acciones de reclamación derivadas del tratamiento o tratamientos realizados.

- * **Principio de proporcionalidad:** este principio exige que los datos sean adecuados, pertinentes y limitados al mínimo necesario en relación con la finalidad para la que van a ser tratados.

Este principio exige definir qué datos son necesarios para cumplir el fin perseguido y poder justificar el uso de cada uno de ellos.

- * **Principio de veracidad y exactitud:** este principio exige tener medidas previstas para conservar los datos actualizados.

Hay situaciones en las que la normativa ya exige una actualización periódica de los datos y en otras el responsable del tratamiento deberá buscar la manera de poder cumplir con esta obligación.

- * **Principio de seguridad de los datos:** garantizar la seguridad de los datos personales y minimizar los riesgos a que estos datos puedan estar expuestos en el tratamiento de estos.

Para cumplir este principio se exige a los responsables del tratamiento adoptar medidas técnicas y además medidas organizativas que permitan garantizar la protección de los datos personales. Crear una cultura de privacidad en la entidad a través de buenas prácticas que motiven a los funcionarios a proteger mejor los datos personales. Como medidas organizativas se pueden trabajar programas de capacitación de los funcionarios públicos con acceso a datos, políticas de mesas limpias, escritorios de ordenadores limpios, incorporar destructoras de papel para los documentos que contengan datos personales, etc.

- * **Principio de transparencia:** este principio exige que la información dirigida al titular de los datos sea en un lenguaje sencillo y claro.

Se debe acompañar la toma y el tratamiento de los datos personales de cláusulas informativas que cumplan todas las exigencias de ser una información clara y sencilla para el usuario, que contenga los datos a que se refiere el artículo 14 del Decreto Ejecutivo 285 de 2021. Y esto con independencia de cuál sea la condición de licitud del tratamiento. De este modo, se debe informar siempre al titular de los datos de lo siguiente:

- La identidad y datos de contacto del responsable del tratamiento y del Oficial de Protección de Datos;
 - la finalidad o finalidades del tratamiento a que se destinarán los datos personales;
 - la condición que legitima el tratamiento;
 - los destinatarios o las categorías de destinatarios de los datos personales, y si están en un tercer país, la condición que legitima la transferencia;
 - el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
 - los derechos que le asisten, así como la forma y mecanismos o procedimientos a través de los cuales podrá ejercerlos;
 - la existencia de decisiones automatizadas, incluida la elaboración de perfiles, y, al menos en tales casos, la información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado;
- * **Principio de confidencialidad:** este principio debe ser entendido desde la óptica de la protección de los datos personales y ser reforzados los deberes de confidencialidad con una mención expresa a los datos personales que son manejados por la entidad;

Implica un compromiso de confidencialidad del responsable del tratamiento o custodio de la base de datos y de todos los usuarios que vayan a tener acceso a los datos en el desarrollo de sus funciones públicas.

- * **Principio de licitud:** principio relacionado con las condiciones de licitud para el tratamiento de los datos;

Todo tratamiento de datos debe estar sujeto a una de las condiciones de licitud que prevé la normativa para ser legal y que se exponen más adelante en esta Guía.

- * **Principio de portabilidad:** como el derecho del titular de los datos a obtener una copia de sus datos personales de manera estructurada en un formato genérico y de uso común.

En el apartado de los derechos de los titulares de los datos, más adelante en esta Guía, se explica con más detalle este derecho de portabilidad.

c. Condiciones de licitud para el tratamiento de los datos personales

La normativa prevé distintas condiciones de licitud conforme a las cuales los datos personales pueden ser objeto de tratamiento. Estas condiciones son:



Cuando el sujeto obligado al cumplimiento es una entidad pública, con carácter general, la condición de licitud para el tratamiento de los datos personales suele ser una obligación legal o el cumplimiento de un interés público.

- * el cumplimiento de una **obligación legal** (art. 6 Ley 81 de 2019 y art. 17.3 Decreto Ejecutivo 285 de 2021), o

Conforme al Decreto Ejecutivo 285 de 2021, la ley que recoja la obligación que implique el tratamiento de los datos debe hacer referencia a los siguientes aspectos:

- la finalidad del tratamiento;
- la determinación del responsable o responsables del tratamiento;
- las limitaciones que rigen la licitud del tratamiento por parte del responsable;
- las categorías de datos objeto de tratamiento;
- los titulares de los datos afectados;
- las entidades a las que se pueden comunicar los datos y los fines de la comunicación; y
- los plazos de conservación de los datos.

De este modo, es importante que el legislador de la República de Panamá, en las normativas que ordenen tratamientos de datos personales, detalle estos aspectos de manera que se genere una mayor cultura y mayor seguridad jurídica en la aplicación de esta condición de licitud por parte de los sujetos obligados a observarlas, sean públicos o privados.

- * el cumplimiento de la salvaguarda del **interés público** (art. 6 Ley 81 de 2019 y art. 17.6 Decreto Ejecutivo 285 de 2021).

Además de estas dos condiciones de licitud que son las más frecuentes, también pueden tener lugar otras condiciones de licitud como son:

- * **relación contractual:** en el ámbito de la relación que exista entre el responsable del tratamiento y el titular de los datos, los tratamientos de datos personales que tengan lugar en la misma se entenderán legitimados por esta relación contractual. (art. 6 Ley 81 y art. 17.2 Decreto Ejecutivo 285);
- * cuando tenga por objeto proteger **intereses vitales** del titular de los datos como pueden ser los casos de urgencia médica o sanitaria, (art. 8 Ley 81 y art. 17.5 Decreto Ejecutivo 285);

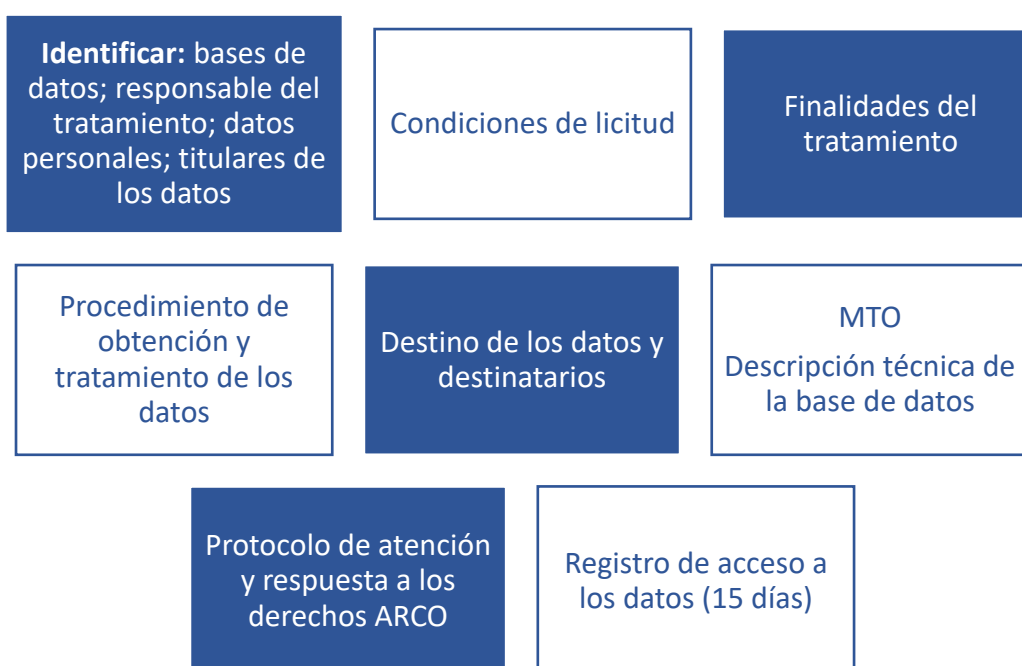
En las relaciones con la Administración Pública, donde no existe una situación de equilibrio entre el responsable del tratamiento (la Administración), y el interesado (el administrado) no sería el consentimiento (art. 6 Ley 81 de 2019 y art. 17.1 Decreto Ejecutivo 285 de 2021) una condición de licitud que se use con frecuencia.

Por último, señalar que la normativa contempla que el interés legítimo no pueda ser utilizado como una condición de licitud por las entidades públicas.

d. Elaborar el registro de las bases de datos

Una de las obligaciones en materia de protección de datos es el elaborar un registro de bases de datos personales. Este registro de las bases de datos transferidas a terceros debe constar por escrito, por cualquier medio, inclusive por medios electrónicos. Debe mantenerse actualizado y estar a disposición de la Autoridad de control cuando ésta lo requiera.

Respecto de cada base de datos se debe indicar la siguiente información:

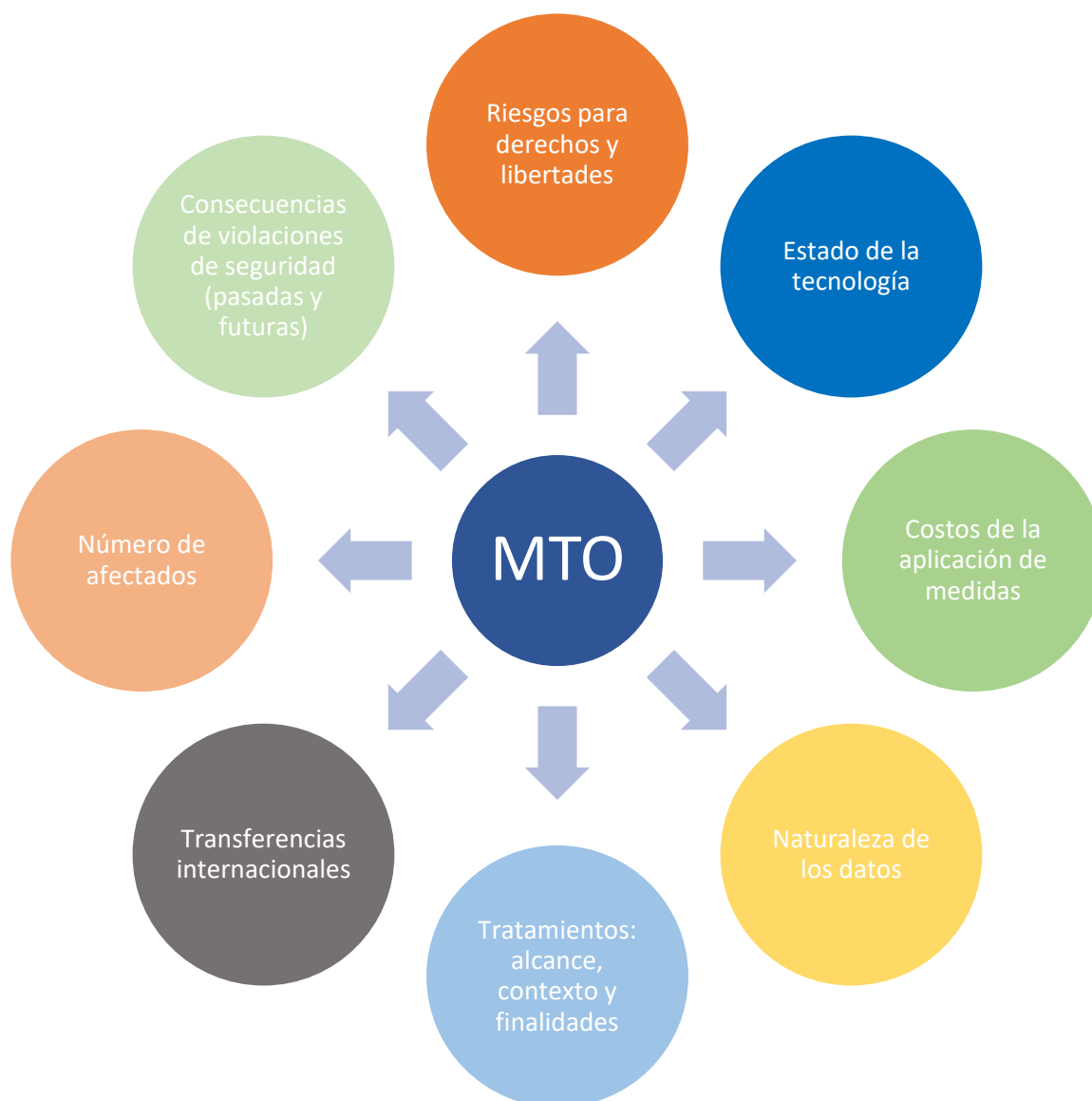


e. Garantizar la seguridad de los datos personales

Conforme al artículo 36 del Decreto Ejecutivo 285 de 2021, las medidas técnicas y organizativas, a las que también se les hace referencia como MTO, deben ser suficientes para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas y servicios de tratamiento de los datos personales.



Para determinar estas medidas técnicas y organizativas (MTO), la normativa indica que se considerarán los siguientes factores:



Las medidas que se decidan adoptar, después de analizados los riesgos del tratamiento, implicarán llevar a cabo una serie de acciones que garanticen el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica.

En el ámbito de las entidades públicas de la República de Panamá se deberá tener presentes, entre otras, las 'Normas generales para la gestión de las TIC en el Estado' elaboradas por la Autoridad Nacional para la Innovación Gubernamental, AIG.

Para terminar con la seguridad de los datos, la normativa establece la obligación de notificar las violaciones de seguridad que representen un riesgo significativo para la protección de los datos personales, a la autoridad de control y a los titulares afectados.

f. Realizar transferencias de datos a terceros con garantías

Cuando el responsable del tratamiento o el custodio de la base de datos, la entidad pública, transfiere datos a un tercero, pueden darse varias situaciones. Cada una de estas situaciones de transferencia de datos tiene unas exigencias legales concretas que debemos cumplir. Es importante recordar que la Ley 81 de 2019 define las transferencias de datos como las intra o extra transfronterizas.

Como regla especial, respecto de los **datos sensibles**, se establece una prohibición de transferencia excepto en los siguientes casos:

- * Autorización explícita del titular de los datos, salvo obligación legal.
- * Necesaria para la salvaguarda de la vida del titular de los datos que se encuentre física o jurídicamente incapacitado, debiendo autorizar la transferencia quien ostente su tutela.
- * Necesaria para el reconocimiento, ejercicio o defensa de un derecho en un proceso con autorización judicial.
- * Para fines históricos, estadísticos o científicos y previa disociación de los datos.

Para el resto de los datos, veamos cada una de las modalidades de transferencia:

- * **Transferencia de datos a terceros:** debe quedar documentada dejando constancia de la solicitud y recepción de los datos que sean objeto de transferencia. (art. 32 y 33 Ley 81 de 2019 y 46 del Decreto Ejecutivo 285 de 2021).

La solicitud de transferencia de datos personales deberá dejar constancia de:

- 1) Quién es el requirente.
- 2) Cuál es el motivo y propósito de la solicitud.
- 3) Qué datos se solicitan.

- 4) Si se cuenta con el consentimiento de los titulares de los datos o si se les ha notificado la transferencia y el destinatario de la misma en base a otra condición de licitud.
- 5)Cuál es el plazo en el que se utilizarán los datos.



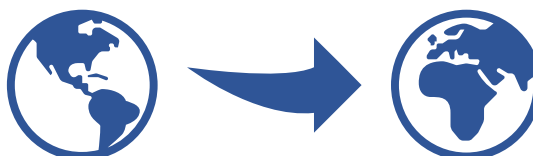
- * **Custodio de la base de datos para la prestación de un servicio:** cuando la transferencia deriva de un mandato del responsable del tratamiento al custodio de la base de datos en el que se establezcan las condiciones para el tratamiento o la utilización de los datos personales. (arts. 10 y 14 de Ley 81 de 2019 y 47 a 49 del Decreto Ejecutivo 285 de 2021).

Se exige que los custodios ofrezcan garantías suficientes en relación con el tratamiento de datos personales. La normativa describe el contenido mínimo que deben tener estos contratos y establece las reglas para las subcontrataciones por parte de un custodio de la base de datos a otros custodios. Es importante atender al contenido mínimo que exige la normativa en estos acuerdos o contratos para garantizar que la protección que los datos personales tienen en el origen lo mantengan en el destinatario de los datos.



- * **Transferencias extrafronterizas de datos:** cuando la transferencia de datos o el mandato a un custodio de la base de datos implica un flujo de datos fuera de las fronteras de la República de Panamá, la normativa prevé una serie de condiciones que deben cumplirse para poder acompañar a los datos de la protección que la normativa confiere. Para ello, se regulan destinos con nivel equivalente de protección y garantías adecuadas a añadir a la transferencia

cuando el destino no cumpla con este nivel de protección. (art. 33 Ley 81 de 2019 y arts. 51 a 53 del Decreto Ejecutivo 285 de 2021)



Como regla especial, en el caso de transferencias solicitadas por las autoridades judiciales competentes, deberán ir acompañadas de una solicitud, debidamente proporcionada al caso concreto, dirigida al responsable del tratamiento o al titular de los datos. Se prohíben así, las solicitudes masivas de información sobre datos personales.

g. Designar un Oficial de Protección de Datos

Para las entidades públicas de la República de Panamá existe una obligación legal de designar un Oficial de Protección de Datos. Conforme a la Ley de Transparencia y Acceso a la Información esta figura coincide con el Oficial de Información. Es importante entender que el Oficial de Protección de Datos requiere de unos conocimientos y una capacitación adecuados y además que tiene unas funciones concretas para contribuir al mejor cumplimiento.

El Oficial de Protección de Datos debe ser designado formalmente y su designación deberá ser notificada a la ANTAI como Autoridad de Control.

Entre las **funciones principales** del Oficial de Protección de Datos encontramos las siguientes:

- * participar en los asuntos relacionados con el cumplimiento de la normativa;
- * informar y asesorar al responsable del tratamiento;
- * ser unidad de enlace con los titulares de los datos; y
- * ser unidad de enlace con la Autoridad de Control.

h. Atender y dar respuesta al ejercicio de los derechos de los titulares de los datos personales

La Ley 81 de 2019 prevé una serie de derechos irrenunciables para el ciudadano que le ayudan a conocer quién, cómo, cuándo, por qué y para qué se están utilizando sus datos personales y así poder reconducir o adecuar el uso de ellos.

Estos derechos son conocidos como derechos ARCO y son Acceso, Rectificación, Cancelación y Oposición, veamos cada uno:

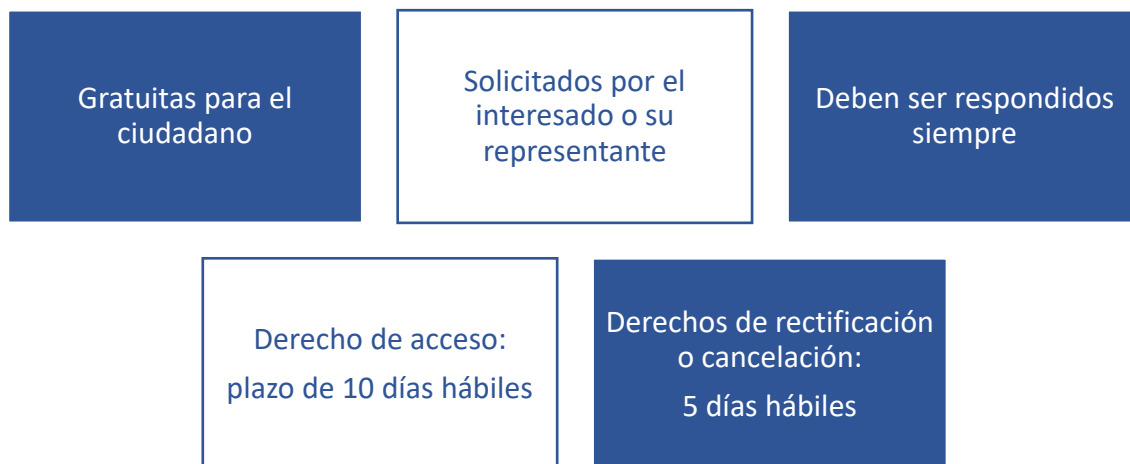
- * **Acceso:** derecho a solicitar el acceso a los datos personales que una institución pública tiene sobre el titular de los datos, a conocer el origen de los datos y el fin para el que fueron recabados. Asimismo, da derecho a obtener una copia de estos.
- * **Rectificación:** derecho a solicitar la corrección de los datos cuando sean incorrectos, irrelevantes, incompletos, inexactos, falsos o impertinentes. El titular de los datos debe indicar en la solicitud qué datos quiere rectificar y acompañar la solicitud de la documentación que demuestre que la rectificación debe ser realizada.
- * **Cancelación:** derecho a solicitar la eliminación de los datos personales cuando sean incorrectos, irrelevantes, incompletos, desfasados, inexactos falsos o impertinentes. El titular de los datos debe indicar en la solicitud qué datos quiere cancelar y acompañar la solicitud de la documentación que demuestre que la cancelación debe ser realizada.
- * **Oposición:** derecho a negarse a que una institución pública utilice sus datos personales siempre que no tenga una causa que lo justifique, por ejemplo, porque los usa en el marco de un contrato, por obligación legal, por interés público porque los usa disociados de su persona, etc.

Se excepciona el ejercicio del derecho de oposición cuando la consulta o solicitud de datos por parte de la entidad gubernamental en el marco del ejercicio de potestades sancionadoras o de inspección, en cuyo caso el ciudadano no podrá impedir, a través de su oposición, que la entidad gubernamental actuante consulte o recabe la documentación que precise.

Además, en la Ley 81 de 2019 se contemplan otros derechos como son:

- * **derecho a la portabilidad:** derecho a recibir una copia de los datos personales, en un formato genérico y de uso común como lo puede ser una impresión o fotocopia, correo electrónico o unidad de almacenamiento. Requiere que el titular haya proporcionado datos personales que hayan sido tratados de forma digital y estructurada.
- * **derecho a no verse sometido a decisiones automatizadas de datos personales:** este derecho debe observarse salvo que el titular de los datos haya consentido, o sea necesario para celebrar o cumplir un contrato o esté contemplado en una ley. Cada vez utilizamos más programas como algoritmos de Inteligencia Artificial que analizan nuestra capacidad crediticia, nuestro perfil profesional, nuestro perfil como consumidor, nuestro perfil de salud, y este derecho nos permite exigir que a partir del análisis automatizado alguien intervenga en la toma de decisiones que se basan en estos análisis para matizar el posible resultado que puede llegar a ser discriminatorio si el programa no está bien configurado o si no se tienen en cuenta datos que el programa no contempla.

Las reglas para la atención y respuesta al ejercicio de derechos son:



En caso de no ser atendida la solicitud de los derechos, el titular de los datos podrá acudir a ANTAI o a la entidad reguladora, en su caso y con carácter previo, para recurrir esta falta de atención por parte del responsable del tratamiento.

Para terminar el apartado de los derechos, debemos referirnos al [derecho a revocar su consentimiento](#) que tiene todo titular de los datos cuando este haya sido la condición de licitud del tratamiento y, por último, al [derecho a la tutela judicial](#), de todo titular de los datos, con independencia de la vía de reclamación administrativa ante la ANTAI, de acudir a los tribunales de justicia para demandar a los responsables del tratamiento o custodios de las bases de datos por los daños y perjuicios causados.

6. ¿Quién es la Autoridad encargada de velar por el cumplimiento de esta normativa?

La Ley 81 de 2019 establece obligaciones para los responsables del tratamiento y mandó a crear la Dirección de Protección de Datos Personales dentro de la Autoridad de Transparencia y Acceso a la Información Pública, ANTAI, Autoridad competente para proteger este derecho de las personas.

Puede visitar su página web en:

www.antai.gob.pa

y la página de la Dirección de Protección de Datos Personales en:

<https://www.antai.gob.pa/direccion-de-proteccion-de-datos-personales/>

7. ¿Cómo actuar ante una denuncia por incumplir la Ley 81 de 2019?

ANTAI a través de su Dirección de Protección de Datos Personales es la Autoridad competente para conocer de las denuncias que puedan derivarse de un uso indebido de los datos personales por parte del responsable del tratamiento y del custodio de la base de datos. El procedimiento administrativo se desarrolla en el marco de la Ley de procedimiento administrativo.

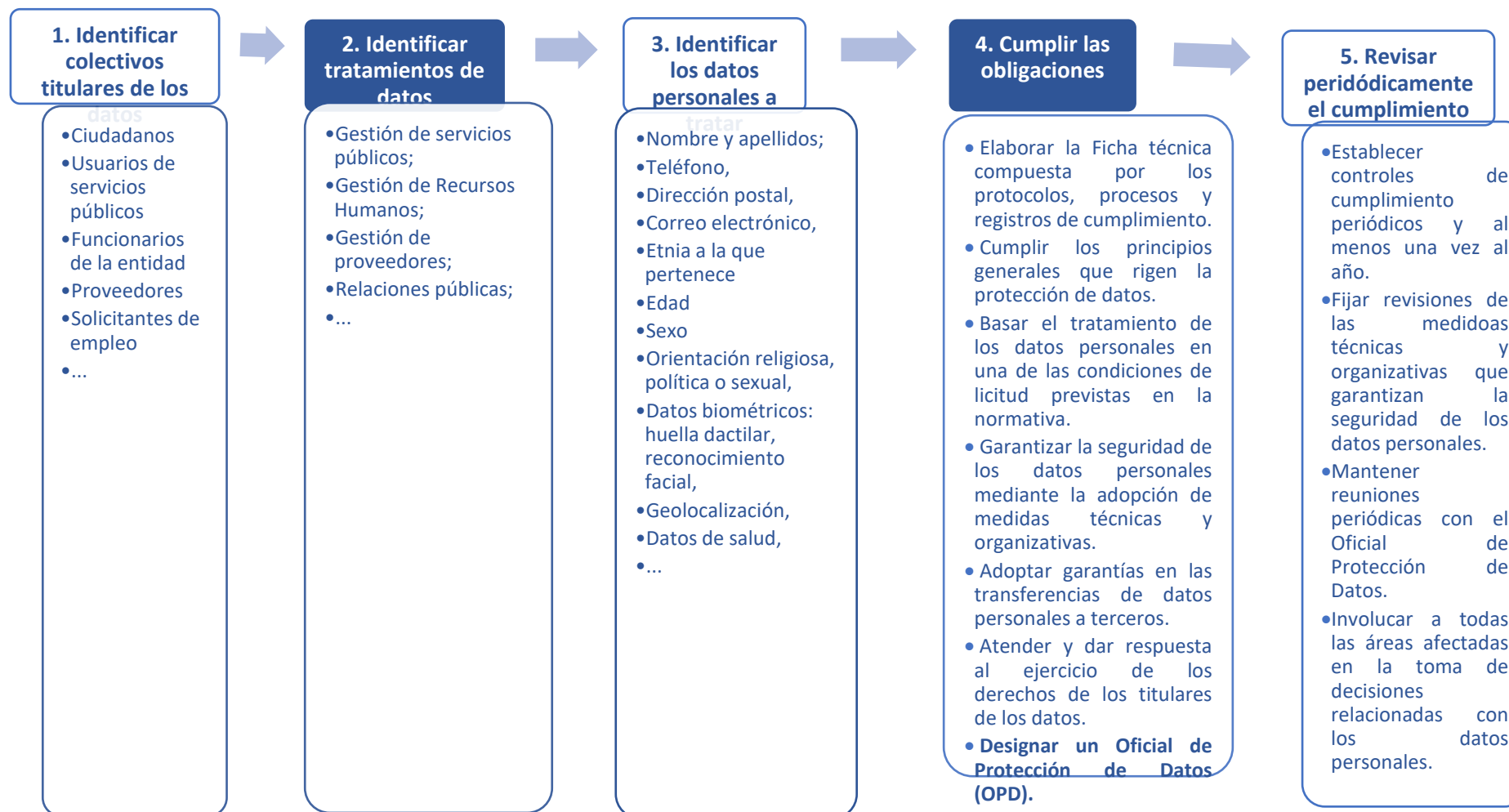
Las decisiones de la Dirección de Protección de Datos Personales serán impugnables mediante recurso de reconsideración en el término de cinco días, a contar desde el día hábil siguiente a la notificación de la resolución de la Dirección, ante la Dirección General de ANTAI en segunda instancia.

Las infracciones previstas en la Ley se clasifican en leves, graves y muy graves. Y las sanciones previstas para las mismas pueden ser bien requerimientos de información por parte de la Autoridad de Control; multas que pueden ir desde los mil hasta los diez mil balboas; clausura de las bases de datos y suspensión o inhabilitación de la actividad de almacenamiento o tratamiento de datos personales de forma temporal o permanente.

El ciudadano puede utilizar distintos canales para enviar su denuncia:

- * Email: protecciondedatos@antai.gob.pa
- * Plataforma de denuncias SmartCID
- * Presencialmente: en las oficinas de ANTAI
- * A través del formulario de denuncia que encontrará en la página web <https://www.antai.gob.pa/direccion-de-proteccion-de-datos-personales/>

Hoja de ruta para el cumplimiento





REPÚBLICA DE PANAMÁ
— GOBIERNO NACIONAL —



**AUTORIDAD NACIONAL
DE TRANSPARENCIA Y
ACCESO A LA INFORMACIÓN**



www.antai.gob.pa