REPÚBLICA DE PANAMÁ
GOBIERNO NACIONAL

AUTORIDAD NACIONAL
DE TRANSPARENCIA Y
ACCESO A LA INFORMACIÓN

# GUÍA PARA CUMPLIR LA NORMATIVA SOBRE

# PROTECCION DE DATOS PERSONALES

# ‘PROTEGIENDO LOS DATOS PERSONALES, SECTOR PRIVADO’

# PROTEGIENDO LOS DATOS PERSONALES

## 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

La privacidad se ha convertido en una prioridad para ciudadanos y empresas. El avance de la economía digital y el valor creciente de los datos personales hace que la economía del dato sea cada vez más exigente con la información personal que necesitamos manejar en nuestros negocios y empresas. En esta guía queremos ayudar a las entidades privadas a poner en valor el esfuerzo que hacen a la hora de cumplir con esta normativa y a conocer la normativa y a tomar conciencia de la necesidad de garantizar la protección de los datos personales que son objeto de tratamiento por ellas en el desarrollo de su actividad económica. Para ello, haremos un recorrido por la normativa para conocer el impacto que esta normativa tiene y explicaremos cuáles son las principales obligaciones que deben cumplir como sujetos obligados y los derechos que deben garantizar a los titulares de los datos en el tratamiento de sus datos personales.

En esta primera guía dirigida al sector privado daremos pautas generales de cumplimiento que sirvan para todas las entidades, sin perjuicio de que, atendiendo al sector de actividad y a los tratamientos de datos personales que se lleven a cabo, se deban tener en cuenta, además, otras pautas de cumplimiento incluso otra normativa especial en la materia.

Cumplir con la normativa sobre protección de datos otorga a las entidades privadas una mayor competitividad frente a otras entidades, nacionales e internacionales, y además supone una mejor reputación frente a consumidores y usuarios.

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 Europa[1] 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, OCDE[2], los Principios actualizados sobre la Privacidad y la Protección de Datos Personales de la Organización de los Estados Americanos, OEA[3], el Reglamento Europeo de Protección de Datos o los Estándares de

[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/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.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 consulta11 de abril de 2023)

Protección de Datos Personales para los Estados Iberoamericanos de la Red Iberoamericana de Protección de Datos[4], RIPD, entre otros.

En la República de Panamá, está regulada 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 y las leyes especiales que lo hagan después de la misma.

Comenzamos…

[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).

## 1. ¿Qué son los 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. Protegemos a las personas a través del tratamiento de sus datos personales. 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.

## 2. ¿Cuál es el ámbito de aplicación territorial de la Ley 81 de 2019?

La Ley 81 de 2019 resulta aplicable, dicta su artículo 5, a las bases de datos que se encuentren en la República de Panamá y a toda entidad pública y toda entidad privada que estén domiciliadas en la República de Panamá respecto de los tratamientos de datos personales que lleven a cabo en el ejercicio de su actividad.

Además, la Ley 81 de 2019 se aplica a todas aquellas actividades de oferta de bienes y servicios que tengan su destino en el mercado panameño. Es decir, podemos exigir el cumplimiento de esta normativa a todas las empresas domiciliadas en la República de Panamá y a aquellas que nos ofrezcan sus productos y servicios desde el extranjero.

## 3. ¿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 las empresas, entidades, profesionales u cualquier organización privada como sujetos obligados son:

* **Responsable del tratamiento:** es la entidad, empresa, organización, comunidad de propietarios, en definitiva, toda entidad privada 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 necesita cuál es el alcance del tratamiento que quiera realizar, así como de los medios que dispone para ello.

Las entidades privadas o las empresas son responsables del tratamiento de las bases de datos que manejan en el desarrollo de su actividad económica. Por ejemplo: base de datos de recursos humanos, de clientes, de potenciales clientes o mercadotecnia, de proveedores, de contabilidad, de agenda de contactos, etc.

Al responsable del tratamiento le corresponde tomar las decisiones relacionadas con el tratamiento de los datos personales. Esto es, qué datos necesita recopilar y con qué finalidad para cumplir con las exigencias que derivan de las relaciones con los clientes, colaboradores o empleados, proveedores, potenciales clientes, solicitantes de empleo, etc.

* **Custodio de la base de datos:** este rol lo ocupa la entidad privada que al 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.

Entre otros ejemplos, encontramos custodios de las bases de datos en las gestorías laborales; en las empresas de tecnología, de desarrollo y mantenimiento de software, de apps o de sistemas basados en inteligencia artificial; en las empresas de almacenaje de documentos; empresas de hosting o alojamiento; en definitiva, en cualquier entidad

que para prestar sus servicios necesita acceder a las bases de datos de las que son responsables otras entidades.

## 4. ¿Cuándo manejamos datos personales?

Una de las primeras tareas que debemos despejar, al abordar la tarea de cumplir con la normativa de protección de datos, es la de identificar los tratamientos de datos personales que realizamos en el desarrollo de nuestra actividad económica, de un lado, y analizar la finalidad o finalidades de tratamiento, así como la condición de licitud del tratamiento, de otro lado.

Las entidades privadas manejan datos personales en el desarrollo de su actividad. 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 clientes, por ejemplo:

* en el registro de entrada y salida de las oficinas o sedes;
* al atender el teléfono de atención al cliente;
* en los contratos de servicios o de productos que les ofrecen;
* en los registros de clientes donde constan sus datos personales, los servicios contratados, los datos de pago, etc.
* en los formularios de toma de datos de sus portales de internet;
* en los dispositivos de seguimiento de usuarios, cookies u otros, que utilizan en las páginas web para analizar el comportamiento de los usuarios;
* al estudiar perfiles de clientes para realizar operaciones de venta cruzada;
* en los formularios en papel que deben completar los clientes, etc.

También tratan datos personales de los colaboradores o empleados. Así, por ejemplo, en el área de recursos humanos tienen los expedientes de los empleados, de los solicitantes de empleo, pueden llevar un registro horario, control de vacaciones y días libres, en definitiva, realizan muchos tratamientos de datos personales que quedan protegidos en el ámbito de esta normativa.

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;

* 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 clientes, proveedores o empleados.

## 5. ¿Qué tratamientos de datos quedan excluidos de la aplicación de la normativa?

La Ley 81 de 2019 exceptúa de su ámbito de aplicación, esto es, no resulta aplicable a los siguientes tratamientos de datos personales:

* Los tratamientos que expresamente se encuentren regulados por leyes especiales o por las normativas que las desarrollen;

Es importante recordar que la Ley 81 de 2019 es un marco general de cumplimiento y que estas leyes especiales deberán respetar los estándares mínimos que establece la Ley, así se menciona en reiteradas ocasiones.

* los que realice una persona natural para actividades exclusivamente personales o domésticas;

La excepción doméstica implica que los tratamientos de datos personales entre particulares fuera de toda relación con la actividad económica o profesional de los mismos, queda fuera de la cobertura de esta ley, sin perjuicio de que el ciudadano tenga otras vías de defensa.

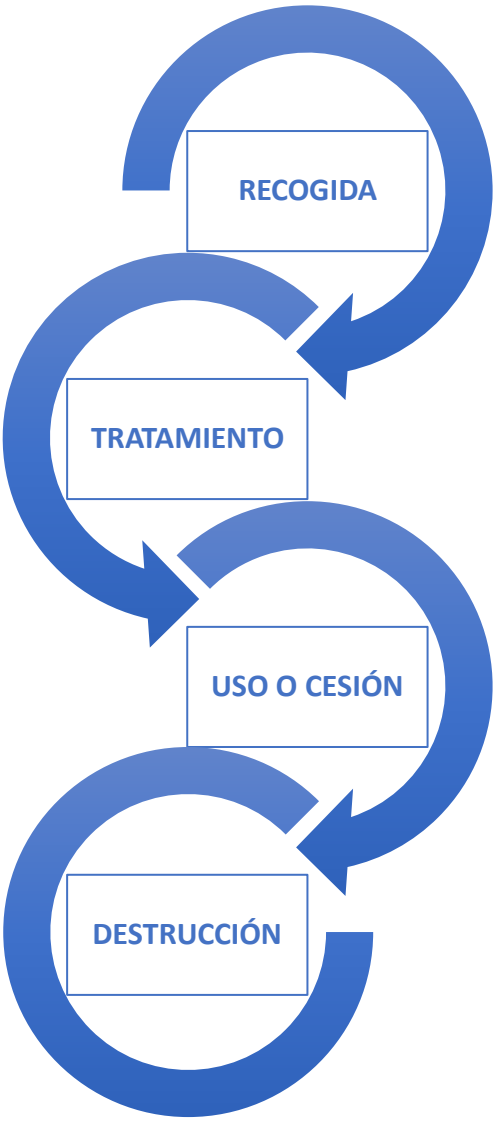
* los que realicen autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales;
* los que se efectúen para el análisis de inteligencia financiera y relativos a la seguridad nacional de conformidad con las legislaciones, tratados o convenios internacionales que regulen estas materias;
* los tratamientos de datos relacionados con organismos internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes ratificados por la República de Panamá;
* los resultantes de información obtenida mediante un procedimiento previo de disociación o anonimización, de manera que el resultado no pueda asociarse al titular de los datos personales.

Si recordamos que los datos personales son los que identifican o hacen identificable a las personas, entendemos bien que estos tratamientos de datos queden excluidos. Es

importante el matiz de que el resultado no pueda llegar a asociarse al titular, hay que tenerlo en cuenta para aplicar la excepción.

## 6. ¿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.

## 7. ¿Qué obligaciones implica el tratamiento de datos personales?

Las obligaciones derivadas de la normativa sobre protección de datos personales varían según el obligado a cumplir sea el responsable del tratamiento o el custodio de la base de datos y también cuando estamos ante responsables solidarios.

En este sentido, lo recomendable es que se tomen un tiempo para analizar los tratamientos de datos que llevan a cabo en calidad de responsable del tratamiento o en calidad de custodio de la base de datos. Una misma entidad realiza tratamientos de datos personales como responsable del tratamiento, por ejemplo, respecto de sus empleados o clientes y a la vez puede estar actuando como custodio de las bases de datos de sus clientes por el servicio que ofrece, por ejemplo, gestoría laboral.

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 dentro del territorio de la República y cuando la transferencia de datos pueda darse fuera del territorio de la República a destinatarios de terceros países.
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).

### 1. Elaborar la Ficha técnica

La Ley sobre Protección de Datos Personales 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:

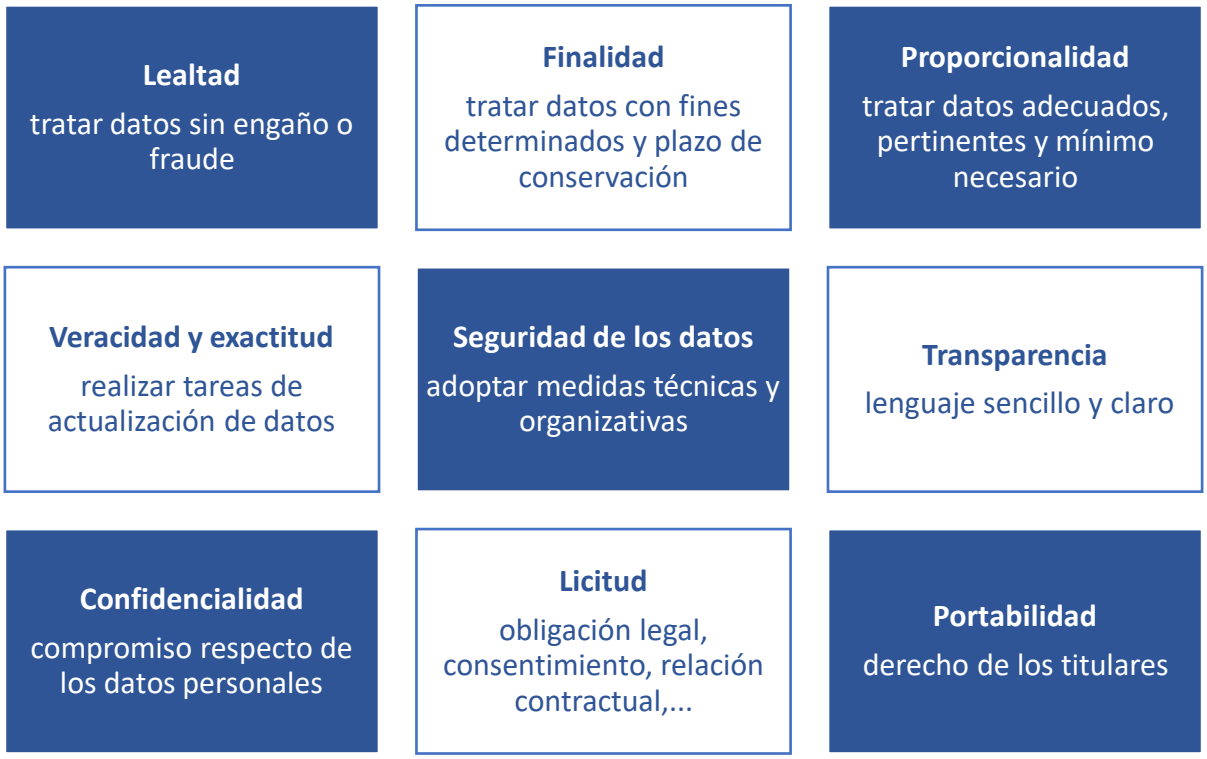

Ficha técnica
Protocolos
Procesos
Registros
Atención y respuesta al ejercicio de derechos ARCO
Cláusulas informativas; contratos con terceros; seguridad de los datos; ...
Canales de entrada de datos
Tratamientos de datos
Almacenamiento de datos,...
Designación del Oficial de Protección de Datos (OPD)
De transferencias de bases de datos
De violaciones de seguridad que afecten a datos personales

Además de elaborar la ficha técnica, el Decreto Ejecutivo 285 de 2021 prevé algunas medidas que se pueden adoptar por responsables del tratamiento y custodios de las bases de datos y que contribuyen al mejor cumplimiento y protección de las personas a través del tratamiento de sus datos. Estas medidas de cumplimiento responsable, entre otras, pueden ser:

* Adoptar mecanismos de autorregulación vinculantes en materia de protección de datos personales.
* Evaluar el impacto que los tratamientos de datos personales pueden tener en los titulares de los datos para minimizar los riesgos.
* Capacitar a los empleados de la entidad que vayan a tener acceso a los datos personales en el desarrollo de su trabajo.
* Designar a un Oficial de Protección de Datos Personales en los términos que veremos más adelante en esta Guía.

## 2. Cumplir con los principios generales en protección de datos personales

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



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

El titular de los datos personales sea cliente, empleado o proveedor, 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, 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. Esto exige que conozcamos los plazos de prescripción de las acciones que puedan ejercitarse por nuestros clientes, empleados o proveedores y que adoptemos medidas para conservar es información o parte de esta para poder atender las posibles reclamaciones, sin perjuicio de que una vez finalizada la relación con estos titulares la información no sea necesario que este accesible o de forma activa en el sistema como el resto de la información.

* 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. Además, nos exige limitar el tratamiento a los datos mínimos necesarios para la finalidad lo que implica que debamos reflexionar sobre qué datos son necesarios y cuáles deseables de cara a decidir cuáles son los datos que finalmente pedimos.

* 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 empleados a proteger mejor los datos personales. Como medidas organizativas se pueden trabajar programas de capacitación en protección de 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, en su caso;
- 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 los empleados en el desarrollo de su trabajo o de los empleados en su relación laboral, por ejemplo;

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

* 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.

* 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.

### 3. Reunir una condición 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:


Veamos cada una de estas condiciones de licitud para conocer qué implicaciones debemos tener en cuenta al basar los tratamientos de datos personales en cada una de ellas:

* Consentimiento: para validar el tratamiento de los datos el consentimiento debe ser previo, prestado de forma inequívoca e informado respecto de los

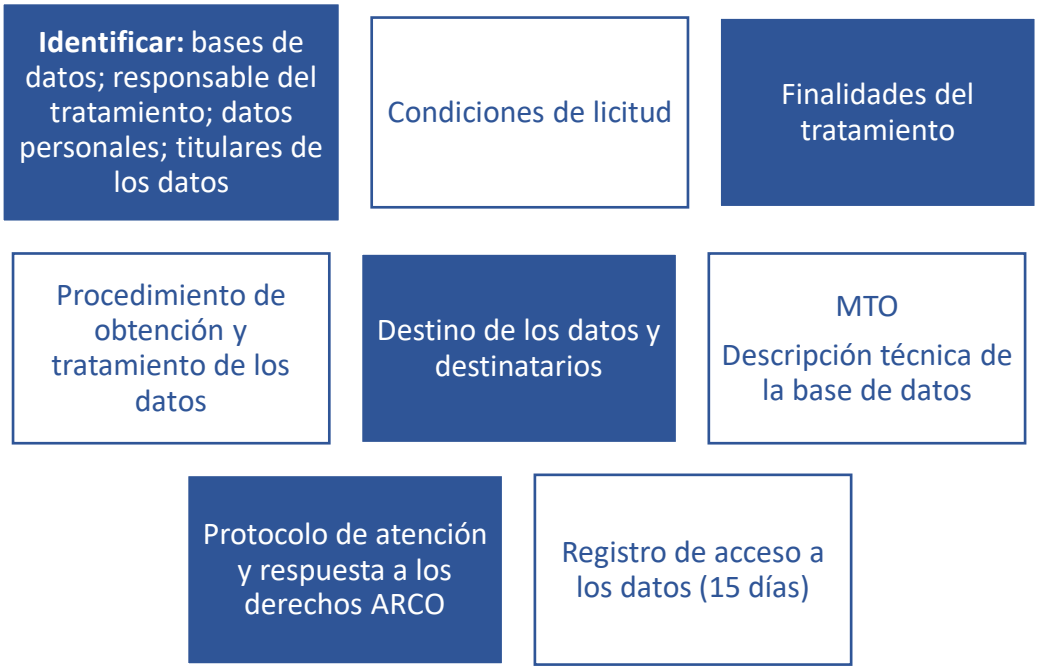
tratamientos de datos y por un medio que permita al responsable probar la trazabilidad de dicho consentimiento. Además, el consentimiento es esencialmente revocable por el titular de los datos sin que esto tenga efectos retroactivos (art. 6 Ley 81 de 2019 y arts. 17.1, 18 y 19 Decreto Ejecutivo 285 de 2021). En el caso de los datos de salud, la ley 81 de 2019, exige que el consentimiento sea previo, irrefutable y expreso.

* 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 de 2019 y art. 17.2 Decreto Ejecutivo 285 de 2021);
* el cumplimiento de una obligación legal (art. 6 Ley 81 de 2019 y art. 17.3 Decreto Ejecutivo 285 de 2021);
* 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 de 2019 y art. 17.5 Decreto Ejecutivo 285 de 2021);
* el cumplimiento de la salvaguarda del interés público (art. 8 Ley 81 de 2019 y art. 17.6 Decreto Ejecutivo 285 de 2021);
* Cuando sea necesario para satisfacer el interés legítimo del responsable del tratamiento o el custodio de la base de datos (art. 8 Ley 81 de 2019 y art. 17.7 Decreto Ejecutivo 285 de 2021)

## 4. Elaborar el registro de las bases de datos

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:



## 5. Garantizar la seguridad de los datos personales

Conforme al artículo 36 del Decreto Ejecutivo 285 de 2021, las medidas técnicas y organizativas 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.

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.

## 6. Realizar transferencias de datos a terceros con garantías

Cuando el responsable del tratamiento o el custodio de la base de datos 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:

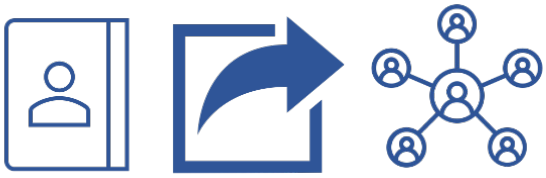
* Autorización explícita del titular de los datos, salvo obligación legal.
* Necesaria para la salvaguarda de la vida del titular de los datos que se encuentre física o jurídicamente incapacitado, debiendo autorizar la transferencia quien ostente su tutela.
* Necesaria para el reconocimiento, ejercicio 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 lose 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.

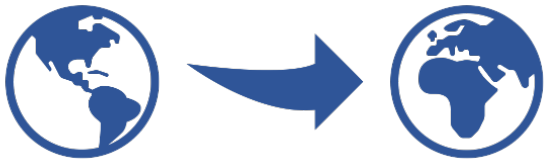


* Custodio de la base de datos para la prestación de un servicio: cuando la transferencia deriva de un mandato del responsable del tratamiento al custodio

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.


* 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 285 de 2021)



## 7. Designar un Oficial de Protección de Datos

Para las entidades privadas de la República de Panamá no existe una obligación legal de designar un Oficial de Protección de Datos. Si bien el Decreto Ejecutivo 285 de 2021 prevé la designación voluntaria de esta figura y si bien algunas entidades reguladoras, como la Superintendencia de Bancos de Panamá, hasta la fecha, ha establecido la necesidad de designar esta figura en el seno de sus entidades reguladas, no se prevé como obligatoria como ocurre para las entidades públicas.

Ahora bien, si queda claro en la normativa que es una medida que puede contribuir a un mejor cumplimiento. En todo caso, se debe saber que si se decide designar voluntariamente a esta figura, en aras a un mejor cumplimiento normativo, se deben

cumplir las mismas exigencias formales que para el Oficial de Protección de Datos obligatorio. Esto es, El Oficial de Protección de Datos debe ser designado formalmente y su designación deberá ser notificada a la ANTAI como Autoridad de Control o, en su caso, a la entidad reguladora correspondiente.

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.

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.

## 8. 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 quieres 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.

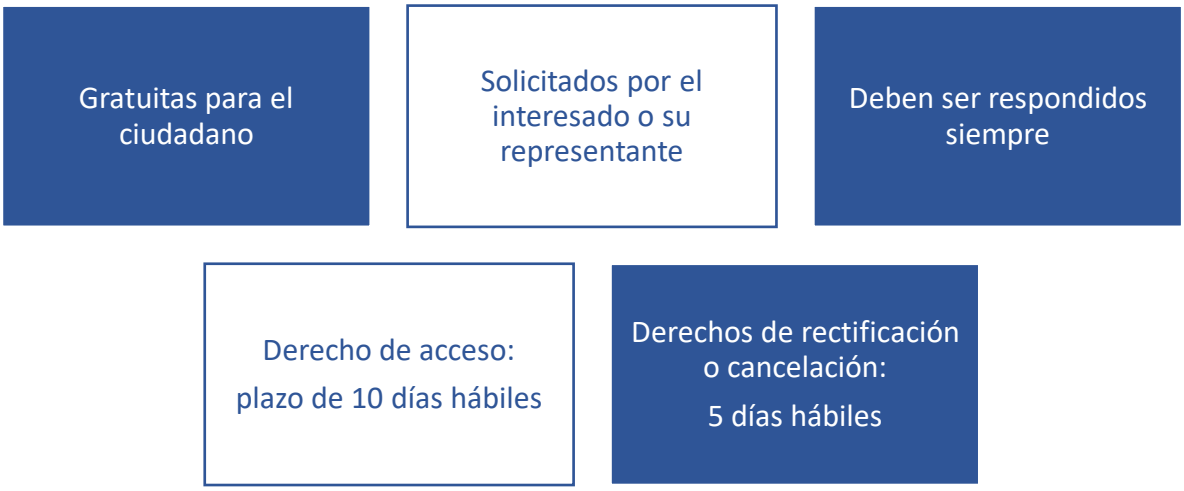
Se excepciona el ejercicio del derecho de oposición cuando la consulta o solicitud de datos por parte de la entidad gubernamental en el marco del ejercicio de potestades sancionadoras o de inspección, en cuyo caso el ciudadano no podrá impedir, a través de su oposición, que la entidad gubernamental actuante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



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, el 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.

## 8. ¿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/

## 9. ¿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.

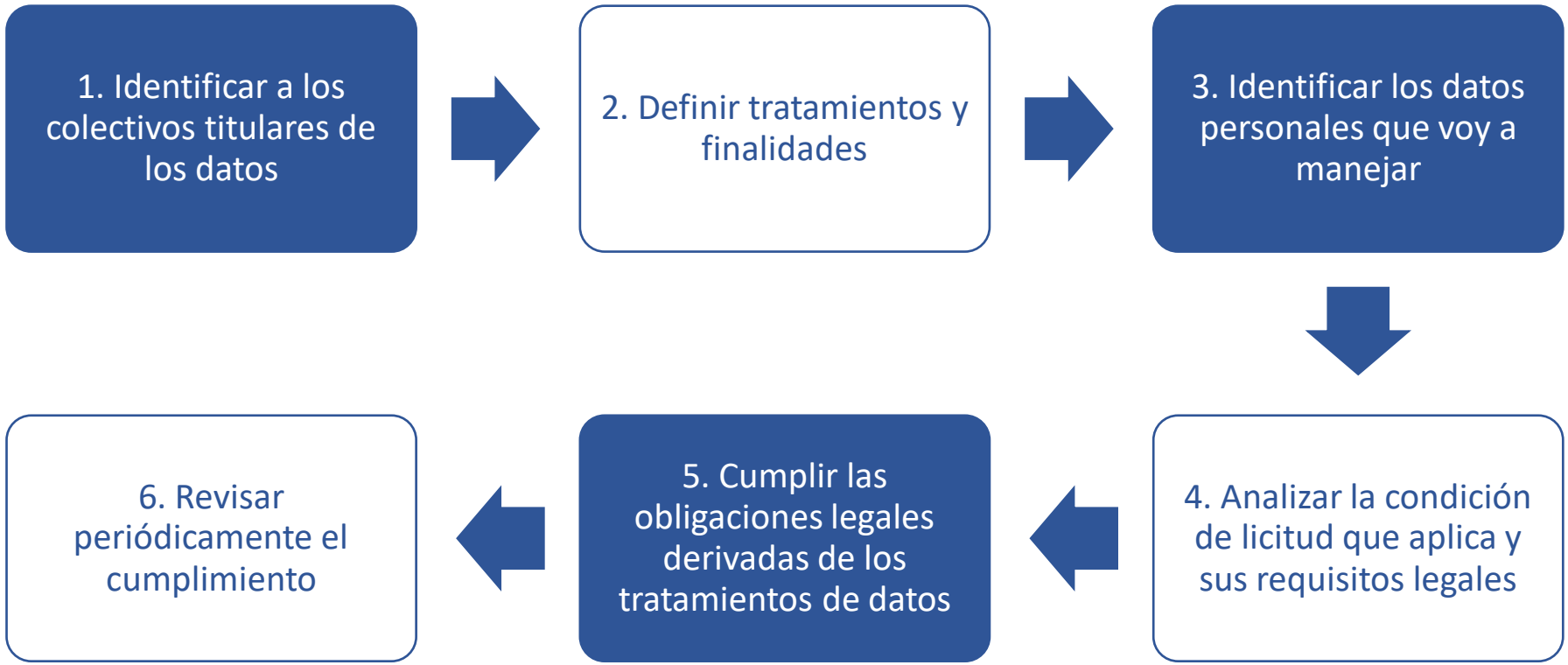
Las decisiones de la Dirección de Protección de Datos Personales serán impugnables mediante recurso de reconsideración en el término de cinco días, a contar desde el día hábil siguiente a la notificación de la resolución de la Dirección, ante la Dirección General de ANTAI en segunda instancia.

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