



Estudio comparativo de Agencias de Protección de Datos Personales

Tomo 1

➤➤ Perú, Paraguay y Colombia





Mayo 2023

Una investigación de la Asociación por los Derechos Civiles (ADC) para el Foro de la Sociedad Civil (FSC) de la Red Iberoamericana de la Protección de Datos (RIPD).

Perú

- Redacción: Luis García Balcarce (ADC)
- Validación: Hiperderecho
- Aval: Autoridad Nacional de Protección de Datos Personales

Paraguay

- Redacción: Luis García Balcarce (ADC)
- Validación: TEDIC

Colombia

- Redacción: Luis García Balcarce (ADC)
- Validación: Fundación Karisma

.....



Es de difusión pública y no tiene fines comerciales. Se publica bajo una licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0). Para ver una copia de esta licencia, visite: <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>

Contenido

Introducción | 4

Diagnóstico del funcionamiento de la agencia de protección de datos personales en Perú | 6

- Funciones
- Dependencias
- Directorio
- Información de Gestión
- Personal
- Legislación ligada a Autoridad Nacional de Protección de Datos Personales
- Proyectos legislativos
- Atribuciones y competencias legales
- Trámites
- Procedimiento de Protección de Derechos
- Transparencia

Diagnóstico del funcionamiento de la agencia de protección de datos personales en Paraguay | 28

- Proyectos legislativos

Diagnóstico del funcionamiento de la agencia de protección de datos personales en Colombia | 34

- Misión
- Visión
- Funciones
- Dependencias
- Información de Gestión
- Personal
- Legislación ligada a Autoridad Nacional de Protección de Datos Personales
- Atribuciones y competencias legales
- Trámites
- Procedimiento de Protección de Derechos
- Transparencia
- Aclaración final

Notas | 51

Introducción

Las agencias de protección de datos personales son organismos públicos que, a grandes rasgos, controlan la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, públicos o privados. No todos los países cuentan con agencias de protección de datos personales y en los que sí lo hacen las agencias revisten características propias y particulares, en término de atribuciones legales, autonomía y competencia, por ejemplo.

La presente investigación, realizada en el marco del trabajo del Foro para la Sociedad Civil (FSC) de la Red Iberoamericana de la Protección de Datos (RIPD), analiza de acuerdo a ciertos ejes diversos aspectos de las agencias de datos personales de diferentes países de Latinoamérica.

Estos ejes son:

- Objetivo general
- Objetivos específicos y acciones
- Información de gestión
- Personal
- Legislación ligada a direcciones nacionales de protección de datos personales
- Proyectos de reforma de leyes de datos personales
- Atribuciones y competencias legales
- Trámites
- Procedimiento de protección de derechos
- Transparencia

La presente investigación cuenta de tres tomos, siendo el tomo I un análisis sobre las direcciones de datos personales de Perú, Paraguay y Colombia. Los tomos II y III se referirán a Argentina, Brasil, Costa Rica, México y Panamá.

La información que contiene este documento fue obtenida a partir de los sitios oficiales de las diferentes agencias de datos personales y de la legislación que las regula. Todos los informes fueron validados por diferentes organizaciones nacionales del país de la agencia y que forman parte del Foro de la Sociedad Civil de la Red Iberoamericana de Protección de Datos. Algunos informes cuentan además con el aval de las propias agencias nacionales, y en los informes que no lo tienen se debe a la falta de información por parte de las mismas.

Este documento resulta una guía fundamental para tener un panorama general de las diferentes agencias de la región.

Diagnóstico del funcionamiento de la agencia de protección de datos personales en Perú

La Autoridad Nacional de Protección de Datos Personales (ANPD) se encuentra en la órbita del Ministerio de Justicia y Derechos Humanos, específicamente depende del Despacho Viceministerial de Justicia¹.



Gráfico 1: Estructura del Ministerio de Justicia y Derechos Humanos en la que se encuentra la Autoridad Nacional de Protección de Datos Personales, dentro de la cual se encuentra la Dirección de Protección de Datos Personales y la Dirección de Fiscalización e Instrucción.

La ANDP vela por garantizar y tutelar el derecho a la protección de datos personales de la ciudadanía. Fomenta una cultura de protección de datos personales y administra el Registro Nacional de Protección de Datos Personales. Además, tiene funciones normativas, resolutivas, fiscalizadoras, sancionadoras, consultivas y de representación, en cumplimiento de la Ley de Protección de Datos Personales (Ley N° 29733) y su reglamento.

La Autoridad Nacional de Protección de Datos Personales (ANPD) cuenta con la Dirección de Protección de Datos Personales y la Dirección de Fiscalización e Instrucción, con las que trabaja conjuntamente.

Funciones

De acuerdo con el artículo 70 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales tiene funciones:

- administrativas
- orientadoras
- normativas
- resolutivas
- fiscalizadoras y
- sancionadoras.

Dependencias

Dirección de Protección de Datos Personales

Es la unidad orgánica que resuelve en primera instancia los procedimientos sancionadores, trilaterales de tutela de derechos en materia de protección de datos personales. Asimismo, administra y mantiene actualizado el Registro Nacional de Protección de Datos Personales. Depende jerárquicamente de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Dirección de Fiscalización e Instrucción

Es la unidad orgánica responsable de fiscalizar el cumplimiento de las obligaciones y prohibiciones establecidas en la Ley de Protección de Datos Personales y su reglamento, así como de iniciar los procedimientos sancionadores por infracción a las disposiciones sobre Protección de Datos Personales e instruir el procedimiento sancionador. Depende jerárquicamente de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Registro Nacional de Protección de Datos

El Registro Nacional de Protección de Datos Personales es el registro de carácter administrativo a cargo de la Autoridad Nacional de Protección de Datos Personales, con la finalidad de inscribir en forma diferenciada, a nivel nacional:

1. Los bancos de datos personales de administración pública o privada, así como los datos relativos a estos que sean necesarios para el ejercicio de los derechos que corresponden a los o las titulares de datos personales.
2. Las comunicaciones de flujo transfronterizo de datos personales.
3. Las sanciones, medidas cautelares o correctivas impuestas por la Autoridad Nacional de Protección de Datos Personales.
4. Los códigos de conducta.

Cualquier persona puede consultar en el Registro Nacional de Protección de Datos Personales la existencia de bancos de datos personales, sus finalidades, así como la identidad y domicilio de sus titulares y, de ser el caso, de sus encargados o encargadas.

Directorio

El directorio de la Autoridad Nacional de Protección de Datos Personales está conformado actualmente por tres personas, una de género masculino -el director general- y dos de género femenino -directoras de protección

de datos personales y de fiscalización e instrucción-. Hay que aclarar que la dirección no obliga ni tiene normativa respecto a cuotas de género.

Información de Gestión

Del balance de gestión 2018 a 2021² publicado por la Dirección Nacional de Protección de Datos Personales surge la siguiente información:

- En el Registro Nacional de Protección de Datos Personales se inscriben los Bancos de Datos Personales (BDP) de administración pública y privada del Perú.
- Entre 2018 y 2021 hubo 11,919 actos de registro. Es de carácter obligatorio realizar los procedimientos de inscripción, modificación y cancelación de BDP.
- Entre esos mismos años hubo 8.097 bancos de datos inscritos. Los BDP contienen información descriptiva sobre los datos personales que recopilan, así como la información necesaria para el ejercicio de los Derechos ARCO³.
- En el 2021 se creó la plataforma virtual para la inscripción de banco de datos personales.
- La ANDP emitió 102 opiniones consultivas, 26 informes jurídicos y 7 opiniones técnicas.
- En el 2018 se recibieron 30 denuncias contra empresas y entidades públicas por el uso inadecuado de datos personales, en el 2019 fueron 52, en el 2020 hubo 142 y en el 2021 llegaron a 138.
- Las fiscalizaciones realizadas para verificar el cumplimiento normativo para que las empresas y entidades públicas respeten el debido tratamiento de datos personales fueron 184 en el 2018, 208 en el 2019, 305 en el 2020 y 335 en el 2021.
- Con referencia a las sanciones impuestas ante infracciones en materia de protección de datos personales, que pueden ser leves, graves o muy graves, la ANPD tiene la facultad de imponer: multas y/o medidas correctivas, para corregir o revertir los efectos de la conducta infractora o evitar que se repita.

- Mediante Resolución Ministerial N°0326-2020-JUS se aprobó la Metodología para el Cálculo de las Multas en materia de Protección de Datos Personales (publicada el 25 de diciembre de 2020 en el Diario Oficial el Peruano) con la finalidad de establecer las pautas y criterios para realizar el cálculo del monto de las multas aplicables por infracciones a la Ley N° 29733, Ley de Protección de Datos Personales y su reglamento, así como lograr una efectiva disuasión de conductas infractoras permitiéndoles a los administrados prever la cuantía de las multas.
- En primera instancia, en el 2018, se fijaron 60 sanciones, en el 2019, 93, en el 2020, 88, y en el 2021, 126.
- En segunda instancia en el 2018 se fijaron 29 sanciones, en el 2019, 43, en el 2020 28, y en el 2021, 44.
- Las multas recaudadas por infracciones en materia de protección de datos personales en el 2018 sumaron un total de 771, 938.58 soles, en el 2019 970,853.90 soles, en el 2020 579,621.67 soles y en el 2021 1,868,135.89 soles.
- En el 2021, la multa impuesta asciende a 6,084.113 soles, la diferencia con la multa recaudada en dicho periodo, radica en que algunas entidades se acogieron al beneficio de reducción de 40% por pronto pago, otras se encuentran en trámite de pago, ejecución coactiva o en vía judicial.
- En primera instancia, se resolvieron en el 2018, 60 solicitudes de tutela de los Derechos ARCO, 67 en el 2019, 69 en el 2020 y 217 en el 2021. En segunda instancia, en el 2018 se resolvieron siete solicitudes, 23 en el 2019, 13 en el 2020 y 28 en el 2021.
- En diciembre del 2020 la ANDP emitió la Directiva para el tratamiento de datos personales mediante sistemas de videovigilancia (Resolución Directoral N° 02-2020-JUS/DGTAIPD del 10 de enero de 2020⁴). A partir de enero de 2020, Perú cuenta con la Directiva de videovigilancia, cuyo objetivo es establecer disposiciones para el tratamiento de datos personales mediante sistemas de videovigilancia con fines de seguridad, control laboral y otros. El tratamiento comprende la grabación, captación,

transmisión, conservación o almacenamiento de imágenes o voces, incluida su reproducción o emisión en tiempo real.

- En lo que se refiere a la difusión de la cultura de la protección de datos personales se realizaron entre 2018 y 2021, 125 charlas informativas y jornadas de sensibilización que beneficiaron a 12.428 personas, entre ellas funcionarias y funcionarios, servidoras y servidores públicos, niños, niñas y adolescentes, actores de sociedad civil y público en general.
- Desde el punto de vista informativo se realizaron tres campañas, como material se publicaron cinco documentos y se abrió un canal audiovisual con videos disponibles para la población en general.

Personal

De la página web de transparencia del Ministerio de Justicia y Derechos Humanos se puede obtener la nómina de personal de dicho Ministerio en general, pero no de la Autoridad Nacional de Protección de Datos Personales en particular⁵. El detalle del personal que conforma la Autoridad Nacional de Protección de Datos Personales en materia de protección de datos personales es el siguiente⁶:

- Abogados y abogadas que realizan propiamente labores en materia de protección de datos personales: 11 personas. De dicho número siete corresponden al género femenino y cuatro al género masculino.
- Ingenieros e ingenieras en materia de protección de datos personales: 1 colaborador del género masculino.

Legislación ligada a Autoridad Nacional de Protección de Datos Personales

De acuerdo con el artículo 70 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales es el órgano de línea encargado de ejercer la Autoridad Nacional de Protección de Datos Personales. La Autoridad Nacional de Protección de Datos Personales se rige por lo dispuesto en la Ley N° 29733, en su Reglamento y en los artículos pertinentes del Reglamento de Organización y Funciones del Ministerio de Justicia.

La Ley N° 29733 tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen. Esta ley se encuentra reglamentada por el Decreto Supremo N° 003-2013-JUS.

El Decreto Legislativo N° 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, es también otra norma ligada a la Autoridad Nacional de Protección de Datos Personales⁷, ya que fortalece el Régimen de Protección de Datos Personales, que a su vez es reglamentado por el Decreto Supremo N° 019-2017-JUS⁸.

En materia de decretos, el Decreto de Urgencia N° 007-2020 aprueba el Marco de Confianza Digital, que establece la obligación de determinados proveedores de servicios digitales de reportar y colaborar con la Autoridad Nacional de la Protección de Datos Personales cuando verifiquen un incidente de seguridad digital que involucre datos personales⁹.

Además, el Decreto Supremo N° 0029-2021-PCM aprueba el Reglamento del Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital¹⁰,

y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo. En esta norma se crea el rol de Oficial de Datos Personales en las entidades públicas y se establece la obligación de las entidades públicas de comunicar a la Autoridad Nacional de Protección de Datos Personales los incidentes de seguridad digital que comprometan datos personales¹¹.

En resoluciones, la Resolución Directoral N° 02-2020-JUS/DGTAIPD aprueba la Directiva N° 01-2020-JUS/DGTAIPD para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia¹².

Y por último, la Directiva de Seguridad de la Información¹³ orienta sobre las condiciones, los requisitos, y las medidas técnicas que se deben tomar en cuenta para el cumplimiento de la Ley de Protección de Datos Personales (Ley N° 29733) y su reglamento, aprobado a través del decreto Supremo N°003-2013-JUS, en materia de medidas de seguridad de los bancos de datos personales.

Proyectos legislativos

Como propuestas legislativas en el 2021 se presentó el proyecto de ley que crea la Autoridad Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, impulsado a través del Ministerio de Justicia y Derechos Humanos¹⁴. Este texto, sindicado con el N° 07870/2020-PE, integra a la Autoridad Nacional de Transparencia y Acceso a la Información Pública, la ANPD y al Tribunal de Transparencia y Acceso a la Información Pública en una sola Autoridad Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Esta iniciativa, que fue presentada al Congreso de la República el 10 de junio de 2021 con carácter de urgencia, integra las actuales dos autoridades y el tribunal administrativo de transparencia en una sola Autoridad Nacional de Transparencia, Acceso a la Información

Pública y Protección de Datos Personales. Esta integración orgánica propone un nuevo estatus de la Autoridad en la estructura del Estado de organismo técnico especializado con personería jurídica propia y recursos presupuestales.

Algunas de las modificaciones propuestas en el proyecto de ley son las siguientes:

- Reconocer el derecho a la portabilidad de datos personales.
- Exigir la institución de un Oficial de Datos Personales para grandes empresas que procesan y almacenan datos personales
- Comunicar incidentes de seguridad que involucren datos personales (obligaciones ambas que ya existen para entidades públicas).

Atribuciones y competencias legales

De acuerdo al art. 32 de la Ley N° 29733 le corresponde a la Autoridad Nacional de Protección de Datos Personales realizar todas las acciones necesarias para el cumplimiento de dicha norma. Esta debe presentar periódicamente un informe sobre sus actividades al Ministro de Justicia. Para el cumplimiento de sus funciones cuenta con el apoyo y asesoramiento técnico de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros, o la que haga sus veces.

Sus atribuciones legales son las siguientes:

- 1.** Representar al país ante las instancias internacionales en materia de protección de datos personales.
- 2.** Cooperar con las autoridades extranjeras de protección de datos personales para el cumplimiento de sus competencias y generar mecanismos de cooperación bilateral y multilateral para asistirse entre sí y prestarse el debido auxilio mutuo cuando se requiera.
- 3.** Administrar y mantener actualizado el Registro Nacional de Protección de Datos Personales.

4. Publicitar, a través del portal institucional, la relación actualizada de bancos de datos personales de administración pública y privada.
5. Promover campañas de difusión y promoción sobre la protección de datos personales.
6. Promover y fortalecer una cultura de protección de los datos personales de niños, niñas y adolescentes.
7. Coordinar la inclusión de información sobre la importancia de la vida privada y de la protección de datos personales en los planes de estudios de todos los niveles educativos y fomentar, asimismo, la capacitación de docentes en estos temas.
8. Supervisar el cumplimiento de las exigencias previstas en esta ley, para el flujo transfronterizo de datos personales.
9. Emitir autorizaciones, cuando corresponda, conforme al reglamento de esta ley.
10. Absolver consultas sobre protección de datos personales y el sentido de las normas vigentes en la materia, particularmente sobre las que ella hubiera emitido.
11. Emitir opinión técnica respecto de los proyectos de normas que se refieran total o parcialmente a los datos personales, la que es vinculante.
12. Emitir las directivas que correspondan para la mejor aplicación de lo previsto en la Ley N° 29733 y en su reglamento, especialmente en materia de seguridad de los bancos de datos personales, así como supervisar su cumplimiento, en coordinación con los sectores involucrados.
13. Promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos personales.
14. Celebrar convenios de cooperación interinstitucional o internacional con la finalidad de velar por los derechos de las personas en materia de protección de datos personales que son tratados dentro y fuera del territorio nacional.
15. Atender solicitudes de interés particular del administrado o general de la colectividad, así como solicitudes de información.
16. Conocer, instruir y resolver las reclamaciones formuladas por

los y las titulares de datos personales por la vulneración de los derechos que les conciernen y dictar las medidas cautelares o correctivas que establezca el reglamento.

17. Velar por el cumplimiento de la legislación vinculada con la protección de datos personales y por el respeto de sus principios rectores.
18. En el marco de un procedimiento administrativo en curso, solicitado por la parte afectada, obtener de los y las titulares de los bancos de datos personales la información que estime necesaria para el cumplimiento de las normas sobre protección de datos personales y el desempeño de sus funciones.
19. Supervisar la sujeción del tratamiento de los datos personales que efectúen el o la titular y el encargado o encargada del banco de datos personales a las disposiciones técnicas que ella emita y, en caso de contravención, disponer las acciones que correspondan conforme a ley.
20. Iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la Ley N° 29733 y en su reglamento, y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento.

Trámites

Para el ejercicio de sus funciones la Autoridad Nacional de Protección de Datos Personales cuenta con diferentes trámites que se pueden hacer online o presencial.

Consultar el Registro Nacional de Protección de Datos Personales¹⁵

Es para consultar la existencia de bancos de datos personales inscritos, sus finalidades, así como la identidad y ubicación de sus titulares o de sus

encargados de acuerdo con el Registro Nacional de Protección de Datos Personales. Se puede acceder a información limitada de manera gratuita, a través de la página de Resultado de Búsqueda de Bancos de Datos Personales inscritos.

También se puede solicitar la información completa por Mesa de Partes virtual, adjuntando el comprobante de pago al Banco de la Nación por 53,10 soles, así como el formulario de consulta con tus datos. Este trámite también se puede hacer presencialmente.

Denuncias por mal uso de datos personales¹⁶

Es un trámite para víctimas o testigos del mal uso de datos personales, ya sea por parte de instituciones públicas o empresas privadas. La denuncia puede ser recibida a través de los canales de atención virtuales o presenciales implementados por el Ministerio de Justicia y Derechos Humanos (MINJUSDH), con el fin de iniciar la fiscalización que corresponda. Esto permitirá determinar los incumplimientos a la Ley de Protección de Datos Personales y, posteriormente, sancionar y aplicar las medidas correctivas adecuadas al caso.

Los requisitos son completar un formulario de denuncia contra la Ley de Datos Personales N° 29733 y presentar documentos que sustenten la acusación.

La denuncia pasará por tres etapas antes de resolverse:

- 1.** Fiscalización de la Dirección de Fiscalización e Instrucción (DFI): en hasta 90 días útiles, la DFI debe emitir un informe recomendando seguir o no un procedimiento administrativo sancionador e informar sobre su decisión por correo electrónico.
- 2.** Evaluación de la DFI: esta área tiene hasta 50 días hábiles para enviar un Informe Final de Instrucción a la Dirección de Protección de Datos Personales.

3. Resolución de la Dirección de Protección de Datos Personales: esta autoridad debe emitir una Resolución Final en un máximo de 20 días hábiles.

Todo este proceso puede durar un máximo de 160 días hábiles. La Resolución es notificada y cualquiera que sea el resultado, la entidad debe explicar detalladamente los motivos de su decisión.

Inscripción de banco de datos en el Registro Nacional de Protección de Datos Personales¹⁷

El Registro Nacional de Protección de Datos Personales (RNPDP) tiene como finalidad inscribir en forma diferenciada a nivel nacional:

- Los bancos de datos personales de administración pública o privada.
- Las sanciones, medidas cautelares o correctivas impuestas por la Autoridad Nacional de Protección de Datos Personales (ANPD).
- Las comunicaciones referidas al flujo transfronterizo de datos personales.

Además, da publicidad de la inscripción de dichos bancos de datos personales, lo que implica que cualquier ciudadano o ciudadana puede consultar este registro. La tasa para inscribir un banco de datos personales es de 75,80 soles.

La ANPD emite la Resolución Directoral correspondiente en un plazo de 30 días hábiles.

Modificar banco de datos en el Registro Nacional de Protección de Datos Personales¹⁸

El trámite puede ser realizado por una persona natural o que forme parte de una entidad privada o pública, y por el o la titular o representante del o la titular de banco de datos personales inscritos en el Registro Nacional de Protección de Datos Personales, que puede modificar la inscripción de los mismos.

El costo es de 61,60 soles y en un plazo de 30 días hábiles, la Autoridad Nacional de Protección de Datos Personales (ANPD) emitirá una Resolución Directoral.

Trámite para el ejercicio de derechos de acceso, rectificación, cancelación y oposición¹⁹

Las personas tienen el derecho a solicitar el acceso, la rectificación, cancelación y oposición (derechos ARCO) de sus datos personales, con el fin de asegurar que sean tratados adecuadamente. Este derecho se da a través de la Ley de Protección de Datos Personales. Previamente se debe solicitar a la entidad privada, pública o persona natural el ejercicio de los derechos ARCO, y esperar respuesta a la solicitud (derecho de acceso: 20 días hábiles; derecho de rectificación, cancelación u oposición: 10 días hábiles).

Ante la falta de respuesta en el plazo o la denegación de la solicitud, se puede presentar el reclamo ante la Autoridad Nacional de Protección de Datos Personales (ANPD). Los requisitos son presentar el formulario (de la web), adjuntar copia de la solicitud enviada a la entidad privada, entidad pública o persona natural, copia de la respuesta denegatoria (si hubiera) y pruebas para sustentar lo solicitado.

La Autoridad Nacional de Protección de Datos Personales (ANPD) resolverá la reclamación dentro del plazo de 30 días hábiles.

Cancelar el banco de datos inscrito en el Registro Nacional de Protección de Datos Personales²⁰

Cualquier persona natural o que forme parte de una entidad privada o pública, y sea titular o representante del o la titular de bancos de datos personales inscritos en el Registro Nacional de Protección de Datos Personales, pueden cancelarlo. El costo es 69,80 soles y la Resolución Directoral correspondiente se emite en un plazo de 30 días hábiles.

Inscribir flujo transfronterizo de datos personales²¹

El trámite lo puede efectuar una persona natural o que forma parte de una entidad privada o pública que sea titular de un banco de datos personales, y envía dichos datos desde fuera del territorio peruano.

Desde el 26 de noviembre de 2018 los formularios de inscripción de banco de datos contienen la comunicación de flujo transfronterizo; no obstante, si se inscribió el banco de datos antes de esa fecha y se indicó la realización de flujo transfronterizo a un determinado país se debe comunicar a la Autoridad Nacional de Protección de Datos Personales (ANPD).

La Autoridad Nacional de Protección de Datos Personales (ANPD) emitirá la Resolución Directoral correspondiente en un plazo de 30 días hábiles.

Denuncias por publicidad no deseada²²

La publicidad no deseada es aquella que llega sin previa invitación, permiso o autorización. Para el envío de publicidad a través de correo

electrónico, mensajes, SMS o WhatsApp, las empresas deben contar con el consentimiento de las personas. Además de otorgar la posibilidad de oponerse a recibirla mediante un medio sencillo y gratuito.

Se puede denunciar la publicidad no deseada cuando se recibe sin consentimiento, si se ejerce el derecho de oposición o retiro del consentimiento y se sigue recibiendo publicidad, o si no se brinda un medio para revocar el consentimiento u oposición.

Otros servicios

Además de los trámites antes enumerados, la Autoridad Nacional de Protección de Datos Personales (ANPD) cuenta con otros servicios adicionales, cómo:

- Solicitud de opinión sobre flujo de datos transfronterizos²³, que son respuestas a consultas formuladas por los y las ciudadanas, así como por personas jurídicas respecto a flujo transfronterizo.
- Solicitud de absolución de consultas de datos personales²⁴, por la que se responden consultas respecto a las opiniones consultivas respecto a la interpretación de las normas de protección de datos personales.
- Consulta de decisiones de la ANPD sobre los derechos ARCO que consta del registro de procedimientos trilaterales y contiene las resoluciones emitidas por la Autoridad en primera y segunda instancia desde el año 2013, así como la consulta de resoluciones emitidas en el marco de los procedimientos sancionadores.

Además, en el sitio web de la ANPD hay una sección con la explicación de los derechos ARCO²⁵ para que las personas conozcan de qué constan y qué hacer ante incumplimientos o violaciones a los mismos.

Procedimiento de Protección de Derechos

De acuerdo al Título VI del reglamento de la Ley N° 29733 existen diferentes procedimientos:

Procedimiento fiscalizador

El procedimiento de fiscalización tendrá por objeto determinar si concurren las circunstancias que justifiquen la iniciación del procedimiento sancionador, con identificación del o la titular del banco de datos personales o del responsable del tratamiento y la presunta comisión de actos contrarios a la Ley N° 29733. Este procedimiento se inicia siempre de oficio como consecuencia de iniciativa directa de la Dirección de Fiscalización e Instrucción, o por denuncia de cualquier entidad pública, persona natural o jurídica.

Procedimiento sancionador

El procedimiento sancionador será promovido siempre de oficio, en atención a un informe de la Dirección de Fiscalización e Instrucción que puede obedecer a una denuncia de parte o a decisión motivada del Director General de Protección de Datos Personales.

Una vez iniciado el procedimiento sancionador, la Dirección de Protección de Datos Personales podrá disponer, mediante acto motivado, la adopción de medidas de carácter provisional que aseguren la eficacia de la resolución final que pudiera recaer en el referido procedimiento, con observancia de las normas aplicables de la Ley del Procedimiento Administrativo General (Ley N° 27444). Asimismo, sin perjuicio de la sanción administrativa que corresponda, se podrán dictar, cuando sea posible, medidas correctivas destinadas a eliminar, evitar o detener los efectos de las infracciones.

Contra la resolución que resuelve el procedimiento sancionador proceden los recursos de reconsideración o apelación dentro de los 15 días de notificada la resolución al administrado.

El recurso de reconsideración se sustentará en nueva prueba y será resuelto por la Dirección de Protección de Datos Personales en un plazo que no excederá los 30 días. El recurso de apelación será resuelto por el Director General de la Dirección de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, debiendo dirigirse a la misma autoridad que expidió el acto que se impugna, para que eleve lo actuado. El recurso de apelación deberá ser resuelto en un plazo no mayor a 30 días.

Infracciones

Las infracciones a la Ley de Protección de Datos Personales (Ley N° 29733), o su reglamento se califican como leves, graves y muy graves y se sancionan con multa de acuerdo al artículo 39 de la citada norma.

- 1.** Son infracciones leves:
 - a.** Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia.
 - b.** Recopilar datos personales que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos.
 - c.** No modificar o rectificar los datos personales objeto de tratamiento cuando se tenga conocimiento de su carácter inexacto o incompleto.
 - d.** No suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios, pertinentes o adecuados para la finalidad para la cual fueron recopilados o cuando hubiese vencido el plazo para su tratamiento. En

estos casos, no se configura la infracción cuando media procedimiento de anonimización o disociación.

e. No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley N° 29733.

f. Dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley N° 29733 y su reglamento.

2. Son infracciones graves:

a. No atender, impedir u obstaculizar el ejercicio de los derechos del o la titular de datos personales.

b. Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del o la titular, cuando el mismo sea necesario conforme a lo dispuesto en la Ley N° 29733 y su reglamento.

c. Realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia.

d. Recopilar datos personales sensibles que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos.

e. Utilizar los datos personales obtenidos lícitamente para finalidades distintas de aquellas que motivaron su recopilación, salvo que medie procedimiento de anonimización o disociación.

f. Obstruir el ejercicio de la función fiscalizadora de la Autoridad.

g. Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley N° 29733.

h. No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley N° 29733, a pesar de haber sido requerido para ello por la Autoridad en el marco de un procedimiento sancionador.

- 3.** Son infracciones muy graves:
- a.** Dar tratamiento a los datos personales contraviniendo las obligaciones contenidas en la Ley N° 29733 y su reglamento, cuando con ello se impida o se atente contra el ejercicio de otros derechos fundamentales.
 - b.** Recopilar datos personales mediante medios fraudulentos, desleales o ilícitos.
 - c.** Suministrar documentos o información falsa a la Autoridad.
 - d.** No cesar en el indebido tratamiento de datos personales cuando existiese un previo requerimiento de la Autoridad como resultado de un procedimiento sancionador o de un procedimiento trilateral de tutela.
 - e.** No cumplir con las medidas correctivas establecidas por la Autoridad como resultado de un procedimiento trilateral de tutela.

Determinación de las multas

Las multas se determinan en función a la Unidad Impositiva Tributaria vigente a la fecha en que se cometió la infracción y, cuando no sea posible establecer tal fecha, la que estuviere vigente a la fecha en que la Dirección General de Protección de Datos Personales detectó la infracción.

Para graduar la sanción a imponerse debe observarse el principio de razonabilidad de la potestad sancionadora reconocido en el numeral 3 del artículo 230 de la Ley del Procedimiento Administrativo General (Ley N° 27444), así como la condición de sancionado reincidente y la conducta procedimental del infractor, en función de la aplicación de la metodología para el cálculo de las multas en materia de protección de datos personales. En caso de que las infracciones continúen, luego de haber sido sancionado, debe imponerse una sanción mayor a la previamente impuesta.

La colaboración con las acciones de la autoridad y el reconocimiento

espontáneo de las infracciones acompañado de acciones de enmienda se considerarán atenuantes.

Acción contencioso-administrativa y hábeas data

Las resoluciones de la Autoridad Nacional de Protección de Datos Personales agotan la vía administrativa. Contra las resoluciones de la Autoridad Nacional de Protección de Datos Personales procede la acción contencioso-administrativa.

Ante incumplimientos o violaciones a la Ley de Datos Personales el afectado debe requerir a la autoridad pública acción con un documento de fecha cierta, que pasados los 10 días y ante la respuesta negativa, la entrega parcial de la información o sin respuesta alguna, el afectado tiene expedito su derecho para acudir al proceso constitucional de hábeas data. El proceso de hábeas data se encuentra regulado junto al proceso de amparo y al de hábeas corpus en Código Procesal Constitucional²⁶.

El artículo 6 del Decreto Legislativo N° 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública prevé que el Tribunal de Transparencia y Acceso a la Información Pública es un órgano resolutorio del Ministerio de Justicia y Derechos Humanos que constituye la última instancia administrativa en materia de transparencia y derecho al acceso a la información pública a nivel nacional. Como tal es competente para resolver las controversias que se susciten en dichas materias.

Transparencia

El Ministerio de Justicia y Derechos Humanos cuenta con un portal web de transparencia²⁷ que cuenta con acceso a información sobre la gestión de dicho ministerio. El portal brinda información detallada sobre presupuesto, personal, planeamiento, contrataciones, participación ciudadana, entre otros. Sin embargo, no permite individualizar por la ANDP. Igualmente a través de él se puede solicitar pedidos de acceso a la información pública para obtener información de gestión de la dirección.

Diagnóstico funcionamiento de la agencia de protección de datos personales en Paraguay

Paraguay no cuenta con una agencia o dirección de datos personales no sólo eso sino que no cuenta con una legislación específica del tema.

Proyectos legislativos

Existe un proyecto de ley de protección de datos personales coordinado por la Coalición de Datos Personales en Paraguay²⁸, un conjunto de organizaciones que realiza investigaciones, eventos y capacitaciones en relación a la protección integral de datos personales²⁹. Esta pregonera por una ley integral de protección de datos personales que apunta a la protección de las personas asegurando las herramientas jurídicas suficientes para garantizar el control sobre su información personal y que los datos recabados sean manejados con confidencialidad, distinguiendo entre los distintos tipos de datos (ej. datos personales y datos sensibles) y los niveles de protección que cada uno requiere.

Por otra parte, señala que la ley debe contar con una autoridad de aplicación independiente que debe velar por el cumplimiento de la legislación y aplicar las sanciones correspondientes. Lo mencionado responde a principios internacionales sobre la materia, pudiendo destacarse como legislación marco el Reglamento General de Protección de Datos que es utilizado en la Unión Europea.

La Coalición trabaja en miras a lograr una legislación que se adecue a estándares internacionales de derechos humanos y que cumpla con todo lo mencionado previamente.

El jueves 28 de enero de 2021 presentaron el borrador final del

anteproyecto de ley en la Cámara de Diputados³⁰. El 19 de agosto de 2021 el presidente de la Cámara de Diputados, Pedro Alliana (ANR-Ñeembucú), recibió al o la titular de la Comisión de Ciencia y Tecnología, Sebastián García (PPQ-Capital), y al vicepresidente del bloque, Edwin Reimer (ANR-Boquerón), quienes, acompañados de representantes de la Coalición de Datos Personales del Paraguay, abogaron por el urgente tratamiento del proyecto de ley “De Datos Personales en Paraguay”³¹.

Se destacó en la reunión que el documento fue trabajado en una mesa interdisciplinaria con miembros de la Coalición y la Comisión de Ciencia y Tecnología, para lograr un marco adecuado de control que proteja los datos de la ciudadanía, garantice el control sobre la información personal y asegure la confidencialidad de los mismos.

El representante de la organización civil aseguró que éste podría ser uno de los proyectos legislativos más importantes de la era democrática, con el que se pretende dar a la ciudadanía la oportunidad de ejercer sus derechos como dueños de sus datos. Agregó que hoy en día la información personal de los paraguayos se encuentra en manos de cualquier empresa pública o privada, y que por ello abundan las estafas electrónicas o avisos enviados por internet.

Autoridad de aplicación en el proyecto de ley

El Capítulo VIII del proyecto de ley regula todo lo referente a la autoridad de aplicación. Define a la Agencia de Protección de Datos Personales como un ente de derecho público y el organismo encargado del control y cumplimiento de las leyes en materia de protección de datos personales con plena autonomía e independencia en el ejercicio de sus funciones.

Compete a la Agencia de Protección de Datos Personales el ejercicio de acciones ante las autoridades nacionales e internacionales y organismos privados o personas vinculadas a la protección de los datos. Le

corresponde así también la asistencia técnica a cualquier institución que lo solicite para la protección de datos personales. Además, la autoridad de control deberá contar con los recursos humanos y materiales necesarios para el cumplimiento de sus funciones.

En cuestión de autoridades, la Agencia de Datos Personales estará conformada por un Director o una Directora y un Subdirector o una Subdirectora, quienes deberán ser de nacionalidad paraguaya, de treinta años cumplidos y deberán contar con antecedentes personales, profesionales y de conocimiento, en particular respecto al ámbito de protección de datos personales, que aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de sus cargos.

Para su elección, el Poder Ejecutivo remitirá a la Cámara de Senadores una lista de tres candidatos a Director o Directora y tres candidatos a Subdirector o Subdirectora, de entre los cuales la Cámara de Senadores elegirá a uno para cada cargo por mayoría absoluta.

El Director o la Directora y el Subdirector o la Subdirectora durarán cinco años en sus cargos, pudiendo ser designados nuevamente. Sólo cesarán por la expiración de su mandato y designación de sus sucesores, o por su remoción en los casos de mal desempeño de sus funciones o la comisión de delitos. Ambos ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño. Sin embargo, podrán ser removidos, por faltas graves e irregularidades cometidas en el ejercicio de sus funciones, por las causas siguientes:

- 1.** El desempeño de un empleo, cargo o comisión distinto de lo previsto en esta ley, excepto la docencia a tiempo parcial.
- 2.** Utilizar en beneficio propio o de terceros la información confidencial de que disponga en razón de su cargo.
- 3.** Ausentarse de sus labores sin mediar permiso, causa de fuerza mayor o motivo justificado.
- 4.** Incapacidad sobrevenida para el ejercicio de su función.
- 5.** Condena firme por delito doloso.

En caso de incurrir en las conductas descritas en el párrafo anterior, se aplicarán análogamente las mismas sanciones establecidas en la Ley 1.626/00 “De la Función Pública”.

Además, en el proyecto la Agencia de Protección de Datos Personales cuenta con suficientes poderes de investigación, supervisión, resolución, promoción, sanción y otros que resulten necesarios para garantizar el efectivo cumplimiento de la presente ley, así como el ejercicio y respeto efectivo del derecho a la protección de datos personales. Las funciones y atribuciones contempladas en son las siguientes:

- 1.** Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente ley y de los medios legales de que disponen para la defensa de sus derechos.
- 2.** Dictar las normas y criterios orientadores que se deben observar en el desarrollo de las actividades comprendidas por el proyecto de ley; específicamente, dictar normas administrativas y de procedimiento relativas a las funciones a su cargo, y las normas y procedimientos técnicos relativos al tratamiento de datos y condiciones de seguridad de las bases de datos.
- 3.** Atender los requerimientos y denuncias interpuestos en relación al tratamiento de datos contemplado en el proyecto.
- 4.** Controlar el cumplimiento de los requisitos y garantías que deben reunir los tratamientos de datos.
- 5.** Solicitar información a las instituciones públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de datos que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados.
- 6.** Imponer las sanciones administrativas que, en su caso, correspondan por violación a las normas.
- 7.** Constituirse en querellante en las acciones penales que se promovieren por violaciones a lo contemplado en el proyecto de ley.

8. Homologar los mecanismos de autorregulación vinculantes y supervisar su cumplimiento.
9. Elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos.
10. Solicitar información a los Delegados de Protección de Datos.
11. Promover acciones de cooperación con autoridades de protección de datos personales de otros países, de carácter internacional o transnacional, pudiendo suscribir acuerdos internacionales administrativos y no normativos en la materia.
12. Preparar informes anuales de gestión sobre sus actividades.
13. Asesorar en forma necesaria al Poder Ejecutivo en la consideración de los proyectos de ley que refieran total o parcialmente a la protección de datos personales.
14. Colaborar con el Ministerio de Tecnologías de la Información y Comunicación en las políticas públicas, investigación y en la gestión de seguridad de la información y ciberseguridad sobre las infraestructuras de bases de datos que contengan datos personales para la adecuada protección de los mismos.

En cuanto a la Directora o Director, le corresponde

1. Representar a la Agencia de Protección de Datos en todos los actos en que ella intervenga.
2. Dirigir las actividades de la institución de conformidad a lo establecido en esta ley y su reglamentación.
3. Controlar y hacer aplicar la ley.
4. Promover la concienciación del público en general y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento de sus datos personales; y asesorar al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento.
5. Brindar información y tratar las reclamaciones de cualquier titular en relación con el ejercicio de sus derechos en virtud de la

presente ley.

6. Desempeñar cualquier otra función relacionada con la protección de los datos personales.

Además, el Director o Directora se debe abstener de cualquier acción que sea incompatible con sus funciones y no participará, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no.

Por su parte, al Subdirector o la Subdirectora le corresponde sustituir al Director o Directora en caso de impedimento, ausencia temporal o vacancia definitiva, asumiendo de inmediato todas sus atribuciones, cooperar con la labor de conformidad a esta ley y supervisar el funcionamiento de las distintas dependencias de la Agencia de Protección de Datos Personales.

En lo referente a los recursos de la Agencia de Protección de Datos Personales se plantea que los mismos estarán constituidos por:

- Los recursos que anualmente le sean destinados en el Presupuesto General de la Nación para el mantenimiento e incremento de sus funciones.
- Los ingresos provenientes de las multas aplicadas en ejercicio de sus potestades sancionadoras establecidas legalmente.
- Los fondos provenientes de convenios y/o acuerdos, créditos otorgados, préstamos, financiamientos, aportes, donaciones, legados, o de cualquier otro concepto, de origen nacional o internacional, siempre que no implique conflicto de interés.

Al momento de la redacción del presente informe la iniciativa se encuentra en su primer trámite constitucional y aguarda tratamiento en el plenario de la institución³².

Diagnóstico del funcionamiento de la agencia de protección de datos personales en Colombia

La Superintendencia de Industria y Comercio protege el derecho fundamental de hábeas data, esto es, conocer, actualizar y rectificar los datos personales. La protección está amparada en la Ley 1.266 de 2008, también conocida como Ley de Hábeas Data, la cual se aplica a todos los datos personales financieros, crediticios, comerciales y de servicios registrados en un banco de datos. En este sentido, la aplicación de esta norma está encaminada a regular el uso de esa información y por tanto otro tipo de datos (por ejemplo, aquellos mantenidos en un ámbito exclusivamente personal o doméstico o los que se incluyen en una historia clínica) se encuentran excluidos de la aplicación de esta norma.

Asimismo, la Ley 1.581 de 2012 establece que la protección será aplicable a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada. Esto será con excepción de las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico, las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo, las bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia, las bases de datos y archivos de información periodística y otros contenidos editoriales, y las bases de datos y archivos regulados por la Ley 79 de 1993 (censos de población y vivienda).

La Superintendencia, a través de la Dirección de Investigación de Protección de Datos Personales, ejerce la vigilancia de los operadores, fuentes y usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países de la misma naturaleza, en cuanto se refiere a la actividad de administración de datos personales.

Además, puede ordenar la corrección, actualización o retiro de datos personales de una base de datos, cuando así se determine dentro de la investigación y, administra el Registro Nacional Público de Bases de Datos.

Misión

La Superintendencia de Industria y Comercio es la autoridad nacional de protección de la competencia, los datos personales y la metrología legal, protege los derechos de los consumidores y administra el Sistema Nacional de Propiedad Industrial, a través del ejercicio de sus funciones administrativas y jurisdiccionales.

Visión

La Superintendencia de Industria y Comercio, en 2030, será reconocida como una entidad ágil, cercana a la ciudadanía, que protege y promueve eficazmente los derechos de los consumidores, el buen funcionamiento de los mercados y el fortalecimiento del sistema de propiedad industrial. Esto, mediante la utilización de tecnología de avanzada, analítica de datos, innovación, mejora continua de procesos, la ampliación de su cobertura, la generación de espacios de participación, la aplicación de mecanismos de prevención y un talento humano comprometido con la honestidad, el respeto, la diligencia y la justicia, la optimización del gasto público y la responsabilidad social.

Funciones

Las funciones de la Delegatura de Datos Personales, que funciona dentro de la SIC, son:

1. Asesorar al Superintendente de Industria y Comercio en la formulación de las políticas en lo que se relaciona con su área.
2. Velar por el cumplimiento de las normas y leyes vigentes y proponer nuevas disposiciones.
3. Apoyar a la Oficina de Servicios al Consumidor y de Apoyo Empresarial en el desarrollo de actividades de divulgación, promoción y capacitación, en los temas de su competencia.
4. Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el o la titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva.
5. Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos.
6. Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personales.
7. Decidir los recursos de reposición y las solicitudes de revocatoria directa que se interpongan contra los actos que expida, así como los de apelación que se interpongan contra los actos expedidos por la Dirección a su cargo.
8. Dirigir las dependencias a su cargo y velar por el eficiente desempeño de las funciones que les corresponden.
9. Recibir y evaluar los informes que le sean presentados e informar periódicamente al Superintendente sobre el estado de los asuntos de sus dependencias y el grado de ejecución de sus programas.
10. Las demás que le sean asignadas y que correspondan a la naturaleza de la dependencia.

Dependencias

Delegado para la Protección de Datos Personales

En Colombia, el derecho fundamental a la Protección de datos Personales está consagrado en el artículo 15 de la Constitución Política y ha sido desarrollado mediante dos leyes estatutarias: la Ley 1.266 de 2008, que regula el hábeas data financiero y que facultó a la SIC para ejercer la vigilancia de los operadores, fuentes y usuarios de información financiera y crediticia no vigilados por la Superintendencia Financiera de Colombia, y la Ley 1.581 de 2012 considerada como el Régimen General de Protección de Datos Personales, aplicable a los datos personales registrados en cualquier base de datos tratados por entidades de naturaleza pública o privada. Esta última norma designó a la SIC como Autoridad de Protección de Datos para garantizar que en el Tratamiento de dicha información se respeten los principios, derechos, garantías y procedimientos dispuestos en la ley y, por supuesto para imponer las sanciones por el incumplimiento a esa disposición.

El Despacho del Superintendente Delegado para la Protección de Datos Personales conocerá de los recursos de apelación que se interpongan frente a las decisiones de las Direcciones de Hábeas Data y de Investigación de Protección de Datos Personales y, además, tiene la labor de tramitar y decidir las solicitudes de Declaración de Conformidad para las Transferencias Internacionales de Datos Personales a países que no cuenten con un nivel adecuado y las solicitudes de Bloqueo Temporal de datos Personales, así como las demás que le asigne la ley.

Dirección de Investigaciones de Protección de Datos Personales

La Dirección de Investigación de Protección de Datos Personales, por su parte, está encargada de adelantar, de oficio o a petición de parte,

investigaciones administrativas sobre posibles incumplimientos al Régimen de Protección de Datos, así como supervisar que, en la práctica, los sujetos obligados - responsables, encargados, fuentes, operadores y usuarios - adopten medidas y políticas eficientes para garantizar el derecho de la ciudadanía a la protección de sus datos personales. Asimismo, en esta Dirección se resuelven los recursos de reposición y en subsidio de apelación que se interpongan frente a las decisiones por ella adoptadas.

Dirección de Hábeas Data

La Dirección de Hábeas Data adscrita a la Delegatura para la Protección de Datos Personales está encargada de recibir y tramitar las quejas o peticiones relacionadas con el amparo del derecho fundamental que tienen las personas a conocer, actualizar o rectificar información que de ellas se haya recogido en bases de datos o archivos. Para esto, desde la Dirección se profieren órdenes que resuelven de fondo las solicitudes de protección del citado derecho fundamental. A su vez, también se resuelven los recursos de reposición y en subsidio de apelación que se interpongan contra dichas órdenes.

Registro Nacional de Bases de Datos

El Registro Nacional de Bases de Datos (RNBD)³³ es el directorio público de las bases de datos sujetas a tratamiento que operan en el país, el cual es administrado por la Superintendencia de Industria y Comercio y de libre consulta para la ciudadanía.

El Gobierno Nacional, mediante el capítulo 26 del Decreto Único 1074 de 2015, reglamentó la información mínima que debe contener el RNBD y los términos y condiciones bajo los cuales se deben inscribir en éste las bases de datos sujetas a la aplicación de la Ley 1.581 de 2012.

Mediante Decreto 090 del 18 de enero de 2018, el Gobierno Nacional modificó el ámbito de aplicación del Registro Nacional de Bases de Datos y creó unos nuevos plazos para que los sujetos que resulten obligados realicen la inscripción de sus bases de datos. Los sujetos que continúan con el deber de registrar sus bases de datos son las sociedades y entidades sin ánimo de lucro que tengan activos totales superiores a 100 mil Unidades de Valor Tributario (UVT) y las entidades de naturaleza pública.

Los plazos establecidos para realizar el registro de las bases de datos son tres: el primero de ellos es para las sociedades y entidades sin ánimo de lucro que tengan activos por más de 610.000 UVT, que deberán registrar sus bases de datos a más tardar el 30 de septiembre de 2018. El segundo plazo es para las sociedades y entidades sin ánimo de lucro que tengan activos totales superiores a 100.000 y hasta 610.000 UVT, quienes tendrán plazo de realizar el registro hasta el 30 de noviembre de 2018. Por último, el tercer plazo corresponde a las entidades públicas, quienes tendrán plazo para registrar sus bases de datos hasta el 31 de enero de 2019.

Las bases de datos que se creen con posterioridad al vencimiento de los plazos ya mencionados, deberán inscribirse dentro de los dos meses siguientes, contados a partir de su creación.

Información de Gestión

A fines de enero del 2022, la Superintendencia de Industria y Comercio, en su rol de autoridad nacional de protección de datos personales, informó en su sitio web que durante el 2021 se recibieron 28.610 quejas ciudadanas (un promedio mensual de 2.384), un 74,49% más respecto a las recibidas durante el 2020³⁴. Según surge de la información brindada, el 90% fue por presuntas infracciones a la ley de *hábeas data* financiero, en donde sobresalió el “incumplimiento del principio de veracidad o calidad

de la información” (los datos no son ciertos o están desactualizados). El 10% restante fue por violaciones a la ley general de protección de datos, en donde la queja principal fue la “falta de autorización para recolectar y usar los datos”.

También se informó que durante el 2021 se logró un incremento del 127% en las multas impuestas con respecto al año anterior, pasando de 76 multas en 2020 a 173 multas en el 2021, por un valor superior a los \$13.500 millones de pesos colombianos.

En 2021 también se impusieron 2.457 órdenes administrativas para que las empresas cumplan con la legislación que protege los datos personales. Además, ese mismo año se expidieron dos guías, con enfoque preventivo, para evitar la vulneración de los derechos de las personas:

- Guía sobre el tratamiento de datos personales en las entidades estatales
- Guía sobre cuidado de identidad digital y protección de datos personales: riesgos sobre el tratamiento de datos personales de niños, niñas y adolescentes

La plataforma de solución directa “SIC Facilita” recibió 5.630 solicitudes de acuerdo entre la ciudadanía y empresas, de las cuales el 82,2% se resolvieron directamente mediante un acuerdo entre las partes. Las principales causas de estas solicitudes fueron:

1. Suplantación de identidad.
2. Falta de comunicación previa al cliente antes del reporte negativ.
3. Reporte erróneo de obligaciones que no están en mora.

Por último, desde el 2021 la Superintendencia de Industria y Comercio ha detentado la presidencia pro tempore de la Red Iberoamericana de Protección de Datos Personales (RIPD).

Personal

El equipo de trabajo principalmente se dedica a:

- Velar por el cumplimiento de la legislación en materia de protección de datos personales.
- Adelantar investigaciones sobre presuntas vulneraciones de la regulación de tratamiento de datos personales.
- Ordenar las medidas que sean necesarias para hacer efectivos los derechos fundamentales al *hábeas data* y al “debido tratamiento de datos personales”.
- El Despacho Superintendente de Industria y Comercio es ocupado por un abogado de género masculino y la Delegatura para la Protección de Datos Personales por una abogada de género femenino.

Del organigrama de la página web de la Superintendencia de Industria y Comercio³⁵ surge que hay una directora al mando de la Dirección de *Hábeas Data* y un director encargado de la Dirección de Investigación de Protección de Datos Personales. En lo que se refiere a los grupos de trabajo, hay un técnico administrativo dentro de la Dirección de *Hábeas Data* y una profesional universitaria en la Dirección de Investigaciones de Protección de Datos Personales.

Legislación ligada a Autoridad Nacional de Protección de Datos Personales

El artículo 15 de la Constitución Política de Colombia consagra el derecho que tienen todas las personas a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Además, el artículo 20 se refiere al derecho a la información

En lo que se refiere a leyes, por una lado está la Ley 1.266 de 2008³⁶, que contiene las disposiciones generales del hábeas data y regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Además, la Ley 1.588 de 2012 desarrolla el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el art. 15 de la Constitución Política; así como el derecho a la información consagrado en el art. 20 de la misma.

En materia de decretos, el Decreto 886 de 2014³⁷ tiene como objeto reglamentar la información mínima que debe contener el Registro Nacional de Bases de Datos, creado por la Ley 1.581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los Responsables del Tratamiento.

Por último, la Circular Única de la SIC³⁸, que en su título V sobre protección de datos personales establece reglas importantes no solo sobre el contenido del derecho de hábeas data, sino también sobre el Registro Nacional de Bases de Datos.

Atribuciones y competencias legales

De acuerdo a los artículo 19 de la Ley 1.581 de 2012 la Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos. Según el art. 21 de esa misma norma sus funciones son:

- 1.** Velar por el cumplimiento de la legislación en materia de protección de datos personales.
- 2.** Adelantar las investigaciones del caso, de oficio o a petición

de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos.

3. Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva.
4. Promover y divulgar los derechos de las personas en relación con el tratamiento de datos personales e implementar campañas pedagógicas para capacitar e informar a la ciudadanía acerca del ejercicio y garantía del derecho fundamental a la protección de datos.
5. Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los responsables del tratamiento y encargados del tratamiento a las disposiciones previstas en la presente ley.
6. Solicitar a los responsables del tratamiento y encargados del tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones.
7. Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos.
8. Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento.
9. Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional.
10. Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personales.

Trámites

De acuerdo al Título V de la Ley 1.266 del año 2008 estos son los trámites y sus procedimientos para realizar con referencia a los datos personales ante los responsables y encargados de datos personales³⁹:

Trámite de consultas

Los o las titulares de la información o sus causahabientes podrán consultar la información personal del o la titular, que repose en cualquier banco de datos, sea este del sector público o privado. El operador deberá suministrarles, debidamente identificados, toda la información contenida en el registro individual o que esté vinculada con la identificación del o la titular.

La petición, consulta de información se formulará verbalmente, por escrito, o por cualquier canal de comunicación, siempre y cuando se mantenga evidencia de la consulta por medios técnicos. Esta será atendida en un término máximo de diez días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la petición o consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su petición, la cual en ningún caso podrá superar los cinco días hábiles siguientes al vencimiento del primer término.

La petición o consulta se deberá atender de fondo, suministrando integralmente toda la información solicitada.

Trámite de reclamos

Los o las titulares de la información o sus causahabientes que consideren que la información contenida en su registro individual en un banco de

datos debe ser objeto de corrección o actualización podrán presentar un reclamo ante el operador, el cual será tramitado bajo las siguientes reglas:

1. La petición o reclamo se formulará mediante escrito dirigido al operador del banco de datos, con la identificación del o la titular, la descripción de los hechos que dan lugar al reclamo, la dirección y, si fuere el caso, acompañando los documentos de soporte que se quieran hacer valer. Transcurrido un mes desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido de la reclamación o petición.
2. Una vez recibida la petición o reclamo completo el operador incluirá en el registro individual en un término no mayor a dos días hábiles una leyenda que diga "reclamo en trámite" y la naturaleza del mismo. Dicha información deberá mantenerse hasta que el reclamo sea decidido y deberá incluirse en la información que se suministra a los usuarios.
3. El término máximo para atender la petición o reclamo será de 15 días hábiles. Cuando no fuere posible atender la petición dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su petición, la cual en ningún caso podrá superar los ocho días hábiles siguientes al vencimiento del primer término.
4. En los casos en que exista una fuente de información independiente del operador, este último deberá dar traslado del reclamo a la fuente en un término máximo de dos días hábiles, la cual deberá resolver e informar la respuesta al operador en un plazo máximo de diez días hábiles. En todo caso, la respuesta deberá darse al o la titular por el operador en el término máximo de 15 días hábiles, prorrogables por ocho días hábiles más. Si el reclamo es presentado ante la fuente, esta procederá a resolver directamente el reclamo, pero deberá informar al operador sobre la recepción del reclamo dentro de los dos días hábiles siguientes a su recibo, de forma que se pueda dar cumplimiento a la obligación de incluir la leyenda que diga "reclamo en trámite" y la

naturaleza del mismo dentro del registro individual, lo cual deberá hacer el operador dentro de los dos días hábiles siguientes a haber recibido la información de la fuente.

5. Para dar respuesta a la petición o reclamo, el operador o la fuente, según sea el caso, deberá realizar una verificación completa de las observaciones o planteamientos del o la titular, asegurándose de revisar toda la información pertinente para poder dar una respuesta completa al o la titular.
6. Sin perjuicio del ejercicio de la acción de tutela para amparar el derecho fundamental del *hábeas data*, en caso que el o la titular no se encuentre satisfecho con la respuesta a la petición, podrá recurrir al proceso judicial correspondiente dentro de los términos legales pertinentes para debatir lo relacionado con la obligación reportada como incumplida.

La demanda deberá ser interpuesta contra la fuente de la información, la cual, una vez notificada, procederá a informar al operador dentro de los dos días hábiles siguientes, de forma que se pueda dar cumplimiento a la obligación de incluir la leyenda que diga “información en discusión judicial” y la naturaleza de la misma dentro del registro individual, que deberá hacerse dentro de dos días hábiles y por todo el tiempo que tome obtener un fallo en firme. Igual procedimiento deberá seguirse en caso que la fuente inicie un proceso judicial contra el o la titular de la información, referente a la obligación reportada como incumplida, y este proponga excepciones de mérito.

En el caso que el o la titular de la información manifieste ser víctima del delito de falsedad personal contemplado en el Código Penal, y le sea exigido el pago de obligaciones como resultado de la conducta punible de la que es víctima, deberá presentar petición de corrección ante la fuente adjuntando los soportes correspondientes. La fuente una vez que reciba la solicitud deberá, dentro de los diez días siguientes, cotejar los documentos utilizados para adquirir la obligación que se disputa, con los documentos allegados por el o la titular en la petición, los cuales se tendrán como

prueba sumaria para probar la falsedad. La fuente, si así lo considera, deberá denunciar el delito de estafa del que haya podido ser víctima.

Con la solicitud presentada, el dato negativo, récord (scorings- score) y cualquier otro dato que refleje el comportamiento del o la titular deberán ser modificados por la fuente reflejando que la víctima de falsedad no es quien adquirió las obligaciones, y se incluirá una leyenda dentro del registro personal que diga “víctima de falsedad personal”.

Las peticiones o reclamos deberán resolverse dentro de los 15 días hábiles siguientes a la fecha de su recibo, prorrogables por ocho días hábiles más. Si en ese lapso no se ha dado pronta resolución, se entenderá, para todos los efectos legales, que la respectiva solicitud ha sido aceptada. Si no lo hiciera, el peticionario podrá solicitar a la Superintendencia de Industria y Comercio y a la Superintendencia Financiera de Colombia, según el caso, la imposición de las sanciones.

Procedimiento de Protección de Derechos

Si el o la titular o sus causahabientes consideran que los datos contenidos en una base de datos deben ser corregidos, actualizados o eliminados, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley 1.266, podrán presentar un reclamo ante el responsable del tratamiento o el encargado del tratamiento, quien tendrá un término de 15 días hábiles para atender la reclamación, contados a partir del día siguiente a la fecha de su recibo.

El o la titular o causahabiente sólo podrá elevar el reclamo ante la Superintendencia cuando:

- Haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento y haya transcurrido un término de 15 días hábiles sin recibir respuesta, o cuando haya recibido una respuesta inadecuada.

- Si ya se elevó la solicitud de consulta o reclamo ante el responsable y/o el encargado del tratamiento y la solicitud no fue atendida.

Los artículos 22, 23 y 24 de la Ley 1.581 de 2012 establecen que la Superintendencia de Industria y Comercio, una vez establecido el incumplimiento por parte del responsable del tratamiento o el encargado del tratamiento, adoptará las medidas o impondrá las sanciones correspondientes. En lo no reglado por la Ley 1.581 y los procedimientos correspondientes se seguirán las normas pertinentes del Código Contencioso Administrativo.

La Superintendencia de Industria y Comercio podrá imponer a los responsables del tratamiento y encargados de tratamiento las siguientes sanciones:

1. Multas de carácter personal e institucional hasta por el equivalente de 2.000 salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;
2. Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.
3. Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.
4. Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

Estas sanciones sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

Las sanciones por infracciones se gradúan atendiendo los siguientes criterios:

1. La dimensión del daño o peligro a los intereses jurídicos tutelados.
2. El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción.
3. La reincidencia en la comisión de la infracción.
4. La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio.
5. La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio.
6. El reconocimiento o aceptación expresas que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

Transparencia

La Superintendencia de Industria y Comercio tiene una sección en su portal web con el presupuesto general de ingresos, gastos e inversión desde el 2012 hasta el 2022⁴⁰. Estos datos son descargables y cuentan con un detalle del presupuesto de ingresos por rentas y recursos de capital. También el presupuesto gastos, que incluye los montos de funcionamiento y de inversión. A su vez, dentro de cada ítem se encuentra detallado cada uno de los conceptos que lo conforman con sus respectivos montos.

De acuerdo al artículo 20 de la Ley 1.581 de 2012, la Superintendencia de Industria y Comercio obtiene sus recursos de lo que le sea destinado en el Presupuesto General de la Nación.

Aclaración final

Para finalizar este informe corresponde aclarar, de acuerdo al artículo 23 de la Ley de Protección de Datos Personales (1.581) de 2012⁴¹, que todo lo referente a los datos personales en poder de entidades públicas el órgano de control es la Procuraduría General de la Nación, que en principio sólo tiene facultades investigativas⁴².

Notas

- 1 <https://www.gob.pe/institucion/anpd/funcionarios> (Clic en “Organigrama”)
- 2 Balance de gestión 2018 a 2021 publicado por la Dirección Nacional de Protección de Datos Personales <https://cdn.www.gob.pe/uploads/document/file/2922144/Transparencia%2C%20Acceso%20a%20la%20Informaci%C3%B3n%20P%C3%BAblica%20y%20Protecci%C3%B3n%20de%20Datos%20Personales.%20Balance%20de%20Gesti%C3%B3n%202018%20-%202021.pdf?v=1647645776>
- 3 Los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) permiten al ciudadano o ciudadana obtener información sobre sus propios datos y el tratamiento que les dan: cuál es su origen, finalidad y de qué forma se están comunicando o compartiendo.
- 4 Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia <https://www.gob.pe/institucion/anpd/informes-publicaciones/1938476-directiva-para-el-tratamiento-de-datos-personales-mediante-sistemas-de-videovigilancia>
- 5 Listado del personal de agosto 2022 https://www.transparencia.gob.pe/personal/pte_transparencia_personal.aspx?id_entidad=131&in_anno_consulta=2022&ch_mes_consulta=08&vc_nombre_funcionario=&vc_dni_funcionario=&ch_tipo_regimen=0&id_tema=32&Ver=&pag=1#.Yz3nP3ZBy5c
- 6 Actualmente, la ANPD cuenta con 20 trabajadores y trabajadoras contratadas como locadores de servicios que realizan funciones permanentes relacionadas a la materia de protección de datos personales. En total, la ANPD cuenta con 32 colaboradores y colaboradoras.
- 7 Texto completo del Decreto Legislativo N° 1.353 <https://cdn.www.gob.pe/uploads/document/file/2998096/Decreto%20Legislativo%20N%C2%BA%201353.pdf.pdf?v=1649268172>

- 8 Texto completo del Decreto Supremo N° 019-2017-JUS <https://cdn.www.gob.pe/uploads/document/file/2998059/Decreto%20SupremoN%C2%BA%20019-2017-JUS.pdf%20.pdf?v=1649268312>
- 9 Texto completo del Decreto de Urgencia N° 007-2020 <https://www.gob.pe/institucion/anpd/normas-legales/2018534-07-2020>
- 10 Texto completo del reglamento de la Ley de Gobierno Digital <https://www.gob.pe/13326-reglamento-de-la-ley-de-gobierno-digital>
- 11 Texto completo del Decreto Supremo N.º 0029-2021-PCM <https://www.gob.pe/institucion/anpd/normas-legales/2018514-0029-2021-pcm>
- 12 Texto completo de la Resolución Directoral N° 02-2020-JUS/DGTAIPD https://cdn.www.gob.pe/uploads/document/file/2011498/RD-N_02-2020.pdf.pdf?v=1626128538
- 13 Texto completo de la Directiva de Seguridad de la información <https://cdn.www.gob.pe/uploads/document/file/1910300/Directiva%20de%20Seguridad%20de%20la%20Informaci%C3%B3n%20Administrada%20por%20los%20Bancos%20de%20Datos%20Personales.pdf?v=1621962867>
- 14 Texto completo del proyecto de ley que crea la Autoridad Nacional Transparencia, Acceso a la Información Pública y Protección de Datos Personales <https://www.gob.pe/institucion/minjus/informes-publicaciones/1958355-proyecto-de-ley-que-crea-la-autoridad-nacional-transparencia-acceso-a-la-informacion-publica-y-proteccion-de-datos-personales>
- 15 Web para consultar el Registro Nacional de Protección de Datos Personales <https://www.gob.pe/9254-consultar-el-registro-nacional-de-proteccion-de-datos-personales>
- 16 Web para denunciar el mal uso de datos personales <https://www.gob.pe/9271-denunciar-el-mal-uso-de-datos-personales>

- 17 Web para inscribir bancos de datos en el Registro Nacional de Protección de Datos Personales <https://www.gob.pe/8060-inscribir-banco-de-datos-en-el-registro-nacional-de-proteccion-de-datos-personales>
- 18 Web para modificar bancos de datos en el Registro Nacional de Protección de Datos Personales <https://www.gob.pe/9251-modificar-banco-de-datos-en-el-registro-nacional-de-proteccion-de-datos-personales>
- 19 Web para realizar el trámite para el ejercicio de derechos de acceso, rectificación, cancelación y oposición <https://www.gob.pe/9269-iniciar-procedimiento-para-el-ejercicio-de-derechos-de-acceso-rectificacion-cancelacion-y-oposicion>
- 20 Web para cancelar el banco de datos inscrito en el Registro Nacional de Protección de Datos Personales <https://www.gob.pe/9252-cancelar-el-banco-de-datos-inscrito-en-el-registro-nacional-de-proteccion-de-datos-personales>
- 21 Web para inscribir el flujo transfronterizo de datos personales <https://www.gob.pe/9253-inscribir-flujo-transfronterizo-de-datos-personales>
- 22 Web para denunciar por publicidad no deseada <https://www.gob.pe/23725-publicidad-no-deseada>
- 23 Web para solicitar una opinión sobre flujo de datos transfronterizos <https://www.gob.pe/9266-solicitar-opinion-sobre-flujo-transfronterizo-de-datos-personales>
- 24 Web para solicitar la absolución de consultas de datos personales <https://www.gob.pe/9264-solicitar-absolucion-de-consultas-de-datos-personales>
- 25 ¿Qué son los derechos ARCO? <https://www.gob.pe/9270-que-son-los-derechos-arco>

- 26 Texto del Código Procesal Constitucional <https://busquedas.elperuano.pe/normaslegales/nuevo-codigo-procesal-constitucional-ley-no-31307-1975873-2/>
- 27 Web del portal de transparencia <http://sistemas3.minjus.gob.pe/transparencia2/transparencia.htm>
- 28 Texto completo del proyecto de ley de protección de datos personales <https://www.datospersonales.org.py/>
- 29 Web de la Coalición de Datos Personales de Paraguay <https://www.datospersonales.org.py/quienes-somos/>
- 30 Presentación del borrador final- Anteproyecto de ley protección de datos personales <https://www.datospersonales.org.py/presentacion-del-borrador-final-anteproyecto-de-ley-proteccion-de-datos-personales-2/>
- 31 Cámara de Diputados. Urgen tratamiento de proyecto que protege datos personales <http://www.diputados.gov.py/index.php/noticias/urgen-tratamiento-de-proyecto-que-protege-datos-personales>
- 32 Ficha técnica del expediente del proyecto de ley de protección de datos personales <http://silpy.congreso.gov.py/expediente/123459>
- 33 Sitio del Registro Nacional de Bases de Datos <https://www.sic.gov.co/registro-nacional-de-bases-de-datos>
- 34 SIC (2022). Más de 28 mil quejas recibió la Superindustria en 2021 por protección de datos personales. <https://www.sic.gov.co/slider/m%C3%A1s-de-28-mil-quejas-recibi%C3%B3-la-superindustria-en-2021-por-protecci%C3%B3n-de-datos-personales#:~:text=BALANCE%20DE%20GESTI%C3%93N%20EN%20PROTECCI%C3%93N,recibidas%20durante%20el%20a%C3%B1o%202020>
- 35 Organigrama de la Superintendencia de Industria y Comercio <https://www.sic.gov.co/organigrama-perfiles-directivos>

- 36 Texto completo de la Ley 1.266 de 2008 <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488#:~:text=por%20la%20cual%20se%20dic-tan,y%20se%20dictan%20otras%20disposiciones>
- 37 Texto completo del Decreto 886 de 2014 <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57338#>
- 38 Texto completo del Título V de la Circular Única de la SIC https://www.sic.gov.co/sites/default/files/normatividad/Titulo%20V%20Proteccion_Datos_Personales.pdf
- 39 Texto completo de la Ley 1266 de 2008 <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488#:~:text=por%20la%20cual%20se%20dic-tan,y%20se%20dictan%20otras%20disposiciones>
- 40 Web con el presupuesto general de ingresos, gastos e inversión desde el 2012 al 2022 <https://www.sic.gov.co/presupuestos-para-la-vigencia>
- 41 Texto completo de la Ley 1.581 de 2012 <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>
- 42 Para más información de este tema: Botero Cabrera, C., Diario El Espectador (2022). La Procuraduría tiene huérfana a la protección de datos personales. <https://www.elespectador.com/opinion/columnistas/carolina-botero-cabrera/la-procuraduria-tiene-huerfana-a-la-proteccion-de-datos-personales/#>



Foro de la Sociedad Civil de la Red Iberoamericana de
Protección de Datos

<https://sociedadcivilripd.org/>