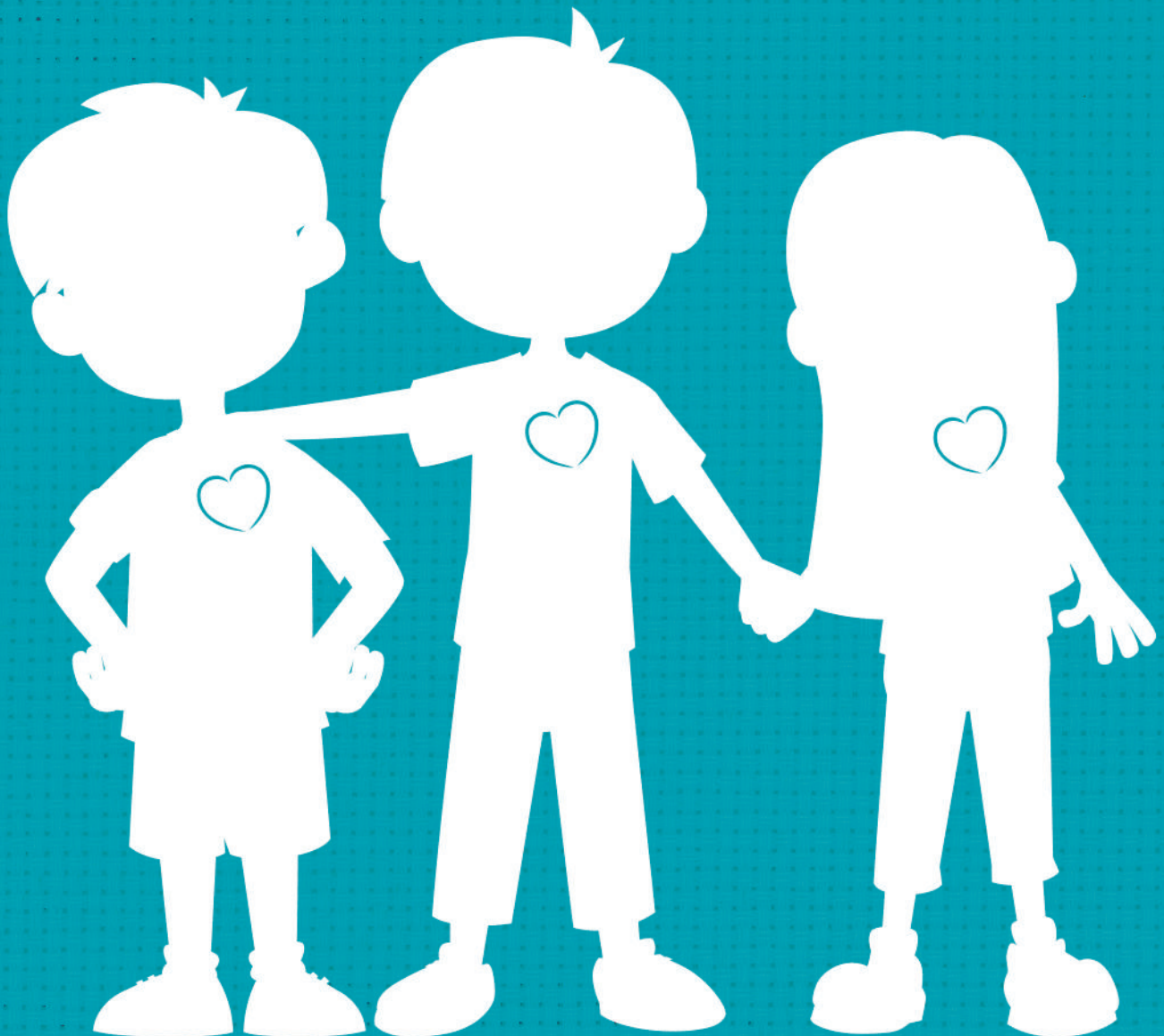


GUÍA PARA EL

TRATAMIENTO DE DATOS PERSONALES DE MENORES DE EDAD





GOBIERNO NACIONAL
★ CON PASO FIRME ★



ANTAI

AUTORIDAD NACIONAL
DE TRANSPARENCIA Y
ACCESO A LA INFORMACIÓN

ÍNDICE

PRESENTACIÓN	1
OBJETIVOS	3
METODOLOGÍA	3
MARCO LEGAL	4
1. REGLAS DE APLICACIÓN GENERAL	6
2. RECOPIACIÓN DE DATOS PERSONALES DE MENORES	8
2.1 ¿Qué categorías especiales de datos existen?	8
2.2 ¿Cuál procedimiento debemos utilizar para su recopilación?	8
3. TRATAMIENTO DE DATOS PERSONALES DE MENORES	10
3.1 ¿Quiénes tienen acceso a la información de las personas menores de edad?	10
3.2 ¿Qué datos se pueden publicar?	10
3.3 Tratamiento de las imágenes de los menores	11
3.4 La cesión de datos de las personas menores de edad	11
4. TRATAMIENTO DE DATOS EN INTERNET	12
4.1 Utilización de Plataformas Educativas por parte de centros de educación	12
5. EJERCICIO DE LOS DERECHOS ARCO	14
5.1 ¿Qué proceso debemos seguir para garantizar el ejercicio los derechos ARCO? Acceso, Rectificación, Cancelación, Oposición y Portabilidad	14
5.2 ¿Cómo proceder cuando se recibe una petición?	15
5.3 ¿Cuál es el contenido de la información que el responsable de los datos deberá proporcionar al titular?	15
6. GLOSARIO	18
7. BIBLIOGRAFÍA	22
8. ANEXOS	23

PRESENTACIÓN

Las organizaciones e instituciones vinculadas a la niñez, desempeñan un papel fundamental en el desarrollo y progreso social de un país, ya que sus funciones promueven la búsqueda de equidad y movilidad social para vivir en la sociedad que queremos.

En materia de niñez debemos recordar la existencia de un principio rector que se pone en valor como premisa esencial, **sea el interés superior del menor o de la menor de edad**. Según la Convención sobre los Derechos del Niño en su artículo 3, esto implica que, *“en todas las medidas concernientes a los niños que tomen las instituciones públicas o privadas de bienestar social, los tribunales, las autoridades administrativas o los órganos legislativos, una consideración primordial, será, el interés superior del niño.”*

El personal institucional y sus equipos administrativos en el ejercicio de sus funciones constantemente tratan datos personales de menores de edad, labor que requiere de la debida diligencia y respeto a su privacidad e intimidad, teniendo siempre presente el interés superior del niño en su sentido más amplio. Los centros educativos, instituciones de servicio social y demás intervinientes en la atención integral de la niñez, realizan una labor incansable por hacer efectiva la gama de derechos fundamentales que cobija a los niños y las niñas. Pero en esta tarea -de manera paralela- se deberá observar el derecho fundamental a la protección de datos personales, que, al no constituir su actividad principal, podría generar dudas respecto a la interpretación e implementación de la regulación nacional en materia de protección de datos personales, en específico, sobre la Ley No. 81 del 26 de marzo del 2019 sobre Protección de Datos Personales y su reglamento, emitido mediante decreto Ejecutivo No. 285 del 28 de mayo de 2021.



El peligro que un inadecuado uso de los datos personales de menores puede producir, no va a tener origen sólo en su comportamiento, sino también en el uso que hagan quienes deben protegerles y representarles, es decir, su familia y los poderes públicos estatales. Por ello, es importante que los menores reconozcan -y se les reconozca de forma expresa- su derecho a la protección de datos personales, y que este reconocimiento vaya aparejado con las mejores prácticas por parte de la institucionalidad y sus representantes.

La Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI), consciente de que, a falta de control de este tipo de datos, podrían derivarse consecuencias cuya afectación impactaría de manera grave el desarrollo personal de niños y niñas, exhorta a las organizaciones y entes responsables a garantizar la vida privada, especialmente de las personas más vulnerables, en este caso niños y niñas. Por lo que la presente guía ofrece reglas de aplicación general para organismos e instituciones de carácter público que en su gestión habitual recopilan y hacen tratamiento de datos de carácter personal de las personas menores de edad.

De acuerdo al marco legal de la República de Panamá en materia de protección de datos personales, se dan pautas que permitan orientar a responsables y encargados del tratamiento de este tipo de datos para generar cultura y alcanzar una adecuada implementación de la Ley No. 81 del 26 de marzo del 2019 sobre Protección de Datos Personales.



OBJETIVOS

Objetivo general

La presente guía ofrece reglas de aplicación general para organismos e instituciones que, en su gestión cotidiana, recopilan y hacen tratamiento de datos personales de personas menores de edad.

Objetivos específicos

- Promover el conocimiento y la concientización institucional con respecto a la Ley No. 81 del 26 de marzo de 2019, sobre Protección de Datos Personales y su reglamento, emitido mediante Decreto Ejecutivo No. 285 de 28 de mayo de 2021.
- Ofrecer información a las instituciones públicas y organismos encargados de brindar atención y servicios a población menor de edad, que les permita hacer una recopilación y tratamiento adecuado de sus datos personales.

METODOLOGÍA

La presente guía se basa en investigación bibliográfica, documental e información obtenida y facilitada por instituciones encargadas de brindar atención y servicios a la población menor de edad.

Los datos cualitativos se han obtenido en un período de cuatro semanas entre noviembre y diciembre, mediante recopilación de información obtenida de repositorios públicos, páginas oficiales de las instituciones públicas y entrevistas a personas funcionarias públicas de instituciones clave en el tema. En este caso, las solicitudes de entrevistas fueron dirigidas a representantes del Ministerio de Desarrollo Social (MIDES), de la Secretaría Nacional de Niñez y Adolescencia (SENNIAF) y al Ministerio de Educación (MEDUCA).

Así, se obtuvo una entrevista con la Dirección Nacional de Informática del Ministerio de Educación (MEDUCA) y también con la Dirección de Desarrollo de la misma institución, por medio de dichas entrevistas fue posible conocer aspectos de suma relevancia para el diseño de la guía, como, por ejemplo, los mecanismos de coordinación interinstitucional para ceder información.

De igual manera, fue de utilidad la información brindada por el Instituto Panameño de Habilitación Especial (IPHE), en entrevista previa, en tanto dicho

ente atiende población menor de edad también.

En el caso de las entrevistas, su duración fue de aproximadamente 30 minutos y fueron realizadas mediante plataformas digitales. El guion de la entrevista se estructuró en seis preguntas, algunas de ellas con sub preguntas a desarrollar, todas las preguntas eran abiertas.

De conformidad con los procedimientos éticos y de salvaguardia, de previo se coordinó con la institucionalidad por parte de la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) para informar sobre el proyecto y la exploración en cuestión.

MARCO LEGAL

Si bien, a nivel internacional no existen normas específicas que regulen el tratamiento de datos de las personas menores de edad, en relación con la protección de los derechos humanos se cuenta con la **Convención sobre los Derechos del Niño**, adoptada por la Asamblea General de las Naciones Unidas, el 20 de noviembre de 1989 y ratificada por la República de Panamá mediante la Ley No. 15 del 6 de noviembre de 1990, donde cabe resaltar el artículo 16 que garantiza que *“1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación. 2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques”*.

La Convención, además, en su artículo 12. 2 reconoce el derechos de los niños a ser escuchados en todo proceso judicial o administrativo que les afecte (De la misma forma, se les garantiza el derecho, en caso de estar privados de libertad, a mantener el contacto con su familia por medio de correspondencia o visitas). En relación con este contacto familiar, si bien la Convención no detalla mucho más, la Asamblea General de las Naciones Unidas aprobó una Resolución estableciendo las Reglas Mínimas de las Naciones Unidas para la administración de justicia a menores (conocida como **Reglas de Beijing**), donde se señaló que cada vez que un menor fuera detenido, la detención debería ser notificada inmediatamente a sus padres o tutores, sin contar con el consentimiento del menor. En el caso de que el contacto suponga peligro a la integridad del menor, habrá que apegarse al principio del interés superior del niño. Por otro lado, con la finalidad de su reinserción y de proteger sus derechos, la misma Convención sobre los Derechos del Niño señala que, *“se respetará plenamente su vida privada en todas las fases del procedimiento”*.

Dichos artículos se inspiran, a su vez, en otras fuentes de derecho

internacional, como lo son, el artículo 12 de la **Declaración Universal de los Derechos del Hombre de 1948**, y el **artículo 17 del Pacto Internacional de Derechos Civiles y Políticos** de 1966, que indican que, “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques” y son aplicables igualmente a las personas menores, en tanto que representan instrumentos jurídicos que garantizan derechos para todas las personas.

Por otro lado, la Constitución Política de Panamá, en su artículo 110, indica que, corresponde primordialmente al Estado el desarrollo de actividades, integrando las funciones de prevención, curación y rehabilitación, entre estas “(...) 3. Proteger la salud de la madre, del niño y del adolescente, garantizando una atención integral durante el proceso de gestación, lactancia, “ crecimiento y desarrollo en la niñez y adolescencia.” (El resaltado no es del original).

En Panamá, además, se cuenta con la Ley No 171 de 15 de octubre de 2020 Ley de Protección Integral a la Primera Infancia y al Desarrollo Infantil Temprano, que establece las bases y directrices técnicas de gestión intersectorial para el desarrollo de una política de Estado en materia de primera infancia y desarrollo infantil. Esta normativa detalla que la ley es aplicable “a la protección integral de los derechos de los niños y niñas en la primera infancia en todo el territorio de la República de Panamá, tanto en el ámbito público como privado o particular”. Asimismo, añade que será de obligatorio cumplimiento en todo el territorio nacional, y serán corresponsables en su ejecución todas las entidades del Gobierno Central, instituciones descentralizadas, gobiernos locales e instituciones privadas y particulares, conforme a sus respectivas competencias.

Por último, pero no menos importante, respecto a los servicios de educación, el marco legal panameño, nos remite a la Ley No. 47 de 1946, Ley Orgánica de Educación, que pone de manifiesto el deber estatal de organizar y dirigir el servicio público de educación, que comprende tanto la educación oficial, impartida por dependencias oficiales, como la educación particular, impartida por personas o entidades privadas.

En concordancia con estas normas e información brindada por las instituciones, habrán de enmarcarse algunas prácticas en materia de tratamiento de datos personales de las y los menores, como, por ejemplo: proveer información para el Programa de Asistencia Social Educativa Universal (PASEU), como medida de justicia social que les permita a los menores recibir un apoyo económico para asistir al sistema educativo, de acuerdo a lo dispuesto por la Ley 148 del 21 de abril del 2020. Asimismo, en relación al programa de asistencia social para familias de escasos recursos, becas y subsidios, se dan cesiones de información entre entidades, como por ejemplo, del Ministerio de

Educación (MEDUCA) hacia Ministerio de Desarrollo Social (MIDES).

En el marco de esta necesaria coordinación institucional legitimada por normas especiales y por la propia Ley de Protección de Datos Personales, se busca promover las mejores prácticas en materia de protección de datos personales, de manera que se continúe trabajando con eficiencia y en respeto absoluto al marco legal vigente.

1. REGLAS DE APLICACIÓN GENERAL

A. Por regla general, el personal institucional y sus equipos administrativos en el ejercicio de sus funciones legalmente otorgadas no necesitan el consentimiento de los titulares de los datos para su tratamiento. Por ejemplo: Los centros educativos en el ejercicio de su función educativa y en la relación al proceso de matrícula del estudiantado, no necesitarán recoger el consentimiento informado. No obstante, a los titulares de los datos o sus responsables, se les debe informar de forma clara, accesible y utilizando un lenguaje sencillo, lo siguiente:

- La identidad del responsable del tratamiento: la institución, administración educativa o el centro,
- La finalidad para la que se recopilan los datos y su licitud, por ejemplo: para el ejercicio de la función educativa, o para dar a conocer las actividades escolares.
- La obligatoriedad o no de proporcionar los datos, así como las consecuencias de la negativa.
- Los destinatarios de los datos.
- Los derechos de los interesados y como ejercerlos.



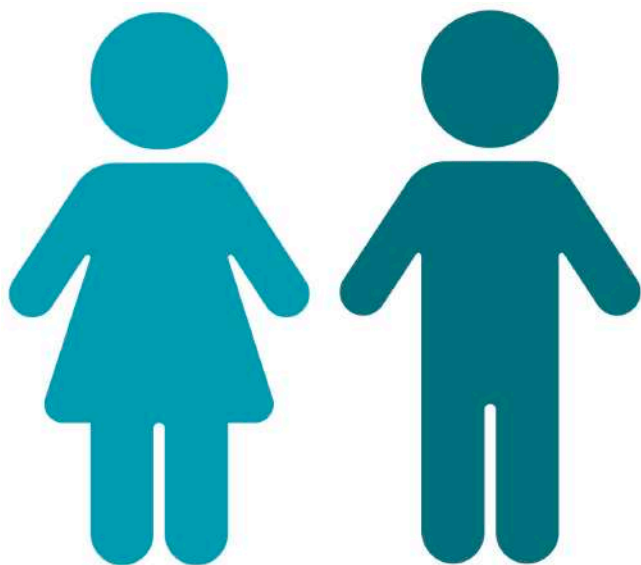
- B. Cuando sea necesario obtener el consentimiento de los menores o de sus padres, para la utilización de sus datos personales por tratarse de finalidades distintas a las mencionadas al momento de la recopilación, se debe informar con claridad de cada una de ellas, permitiendo a las personas interesadas oponerse cuando así lo consideren.
- C. Las TICs son herramientas fundamentales para la gestión del conocimiento por lo que los organismos e instituciones, así como los centros educativos deben conocer las aplicaciones que vayan a utilizar, su política de privacidad y las condiciones de uso antes de utilizarlas o adquirirlas, debiendo desestimar las que no brinden información sobre el tratamiento de los datos personales que realizan.
- D. Cuando las instituciones públicas, especialmente los centros educativos organicen actividades (festivales artísticos, fiestas de fin de curso, eventos deportivos) a los que asistan los familiares de los alumnos, se recomienda informarles mediante avisos o carteles, de la posibilidad de grabar imágenes y los usos que se les dará a dichos datos.
- E. La existencia de un principio rector de la actuación administrativa (interés superior del menor) no constituye en todos los supuestos título legal habilitante para la cesión de datos relativos a personas menores de edad entre las administraciones públicas.
- F. Cuando distintos órganos estatales, organismos nacionales o internacionales soliciten acceso a bases de datos personales de personas menores de edad, la institución responsable de los datos, deberá revisar si se cuenta con norma habilitante para realizar dicha cesión, o bien, verificar si se encuentra dentro de alguno de los supuestos de excepción de acuerdo a los artículos 6 y 8 de la Ley No. 81 del 26 de marzo del 2019, de protección de datos personales, respectivamente. (ver anexo 1).
- G. De realizarse cesión de datos en apego al marco legal nacional, el organismo u ente receptor de dicha información, deberá firmar un convenio de confidencialidad y seguridad de la información, así como contar con protocolos de protección de datos y seguridad de la información que sean verificables por parte de la institución responsable del tratamiento de datos personales. En estos casos, será medular también que las instituciones cuenten con protocolos de pseudoanonimización, con el fin de transferir datos que impidan identificar a las personas y con ello disminuir una serie de riesgos vinculados a la niñez, como lo son el tráfico de órganos, secuestro y crimen organizado de menores.

2. RECOPIACIÓN DE DATOS PERSONALES DE MENORES

2.1. ¿QUÉ CATEGORÍAS ESPECIALES DE DATOS EXISTEN?

De acuerdo a la Ley No. 81 del 26 de marzo del 2019 sobre Protección de Datos Personales, un dato personal es cualquier información concerniente a personas naturales, que las identifica o las hace identificables. Algunos de los datos personales son especialmente sensibles por revelar circunstancias de las personas sobre su esfera más íntima y por ello requieren que se les preste especial atención y se adopten las medidas técnicas y organizativas necesarias para evitar que su tratamiento origine lesiones en los derechos y libertades de los titulares de los datos. De manera enunciativa se consideran sensibles los datos personales que puedan revelar aspectos como:

- Origen racial o étnico
- Creencias o convicciones religiosas, filosóficas y morales
- Afiliación sindical; opiniones políticas
- Datos relativos a la salud, a la vida, a la preferencia u orientación sexual
- Datos genéticos o datos biométricos



Ejemplos de datos sensibles en el ámbito educativo:

- a) Tratamiento de datos relativos a la salud física o mental de las personas estudiantes, incluida la prestación de servicios de atención sanitaria que revelen información sobre su estado de salud.
- b) Recopilación de datos de salud de los alumnos para el ejercicio de la función educativa, discapacidades físicas o psíquicas, por ejemplo, del síndrome Trastorno por Déficit de Atención e Hiperactividad (TDAJH).
- c) También son datos de salud los contenidos en los informes psicopedagógicos elaborados por los departamentos de orientación o psicología de la institución.

2.2 ¿CUÁL PROCEDIMIENTO DEBEMOS UTILIZAR PARA SU RECOPIACIÓN?

Los datos personales que se recojan deben ser únicamente los que requiera la institución para dar la atención o servicio que necesite el o la menor de edad. De modo que habrá que recolectar únicamente la cantidad de datos personales que sea necesaria, proporcional y pertinente para llevar a cabo la atención.

Para ello será importante contar con formularios prediseñados, para que el personal técnico sepa en cada ocasión qué información debe completar, solicitando a la persona aquellos datos que sean estrictamente necesarios para resolver la necesidad concreta.

Por ejemplo, la Ley Orgánica de Educación, en concordancia con la Ley No. 81 del 26 de marzo del 2019, sobre Protección de Datos Personales, legitiman a los centros educativos para recabar y tratar los datos de los alumnos y de sus padres/tutores, incluyendo también las categorías especiales de datos (como los de salud o de religión) cuando fuesen necesarios para el desempeño de la función docente. Sin embargo, habrá que tener en cuenta algunas consideraciones:

- Los datos personales no podrán usarse para fines diferentes al educativo.
- El profesorado y resto del personal que acceda a los datos personales de los y las menores o de sus familias, estará sometido al deber de confidencialidad.

Además, se pueden recabar datos de salud en la medida en que sean necesarios para el ejercicio de la función educativa. Se pueden distinguir los siguientes momentos:

- **Al momento de hacer de matrícula:** discapacidades, padecimientos o enfermedades crónicas, TDAH, intolerancias alimentarias o alergias.
- **Durante el curso escolar:** el tratamiento médico que reciba el o la menor a través del servicio médico o de enfermería del centro o los informes de centros sanitarios a los que se les haya trasladado como consecuencia de accidentes, indisposiciones sufridas en el centro o los informes de los equipos de orientación psicopedagógica.

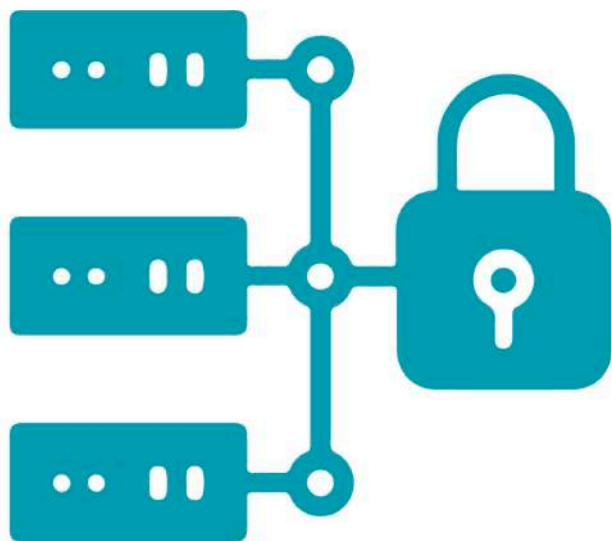
3. TRATAMIENTO DE DATOS PERSONALES DE MENORES

3.1 ¿QUIÉNES TIENEN ACCESO A LA INFORMACIÓN DE LAS PERSONAS MENORES DE EDAD?

Las instituciones públicas y organismos que traten datos personales de menores de edad, disponen de datos cuya naturaleza es diversa: identificativos, académicos, familiares, económicos, sociales, de salud, a los que podrán acceder sólo las personas que lo necesiten para ejercer la función legalmente otorgada.

En este sentido, es de relevancia señalar que, en el caso de los centros educativos, los profesores deben conocer y, por tanto, acceder a la información de salud de sus alumnos, para garantizar la adecuada atención y con ello

su derecho fundamental a la educación. Por ejemplo: Respecto a discapacidades auditivas, físicas o psíquicas, trastornos de atención, TDAH, padecimientos o enfermedades crónicas.



Igualmente, deberán conocer la información relativa a las alergias, intolerancias alimentarias o la medicación que pudiera requerir el o la estudiante para poder prestar el adecuado cuidado dentro del centro educativo o bien, en relación a la coordinación que la entidad educativa haga con instituciones que prestan servicios sociales:

atención a la salud, subvenciones y becas, por ejemplo.

Respecto de la solicitud de información por parte de los responsables o padres de las personas menores en razón de su interés legítimo, estos podrán/deberán ser informados de las distintas situaciones en todo momento.

3.2 ¿QUÉ DATOS SE PUEDEN PUBLICAR?

Cuando se requiera informar sobre la admisión o inclusión, sea a algún centro educativo o programa de formación, asistencia social, beneficio, entre otras; se podrá publicar la información. No obstante, la publicidad deberá realizarse de manera que no suponga un acceso indiscriminado a los datos personales de la persona menor de edad, por ejemplo: publicando en una página web de acceso restringido accesible solo para quienes hayan solicitado la admisión o inclusión. Esta publicación deberá contener únicamente el resultado, no resultados parciales que puedan revelar datos o información sensible o poner de manifiesto la capacidad económica u otros datos de la familia.

3.3 TRATAMIENTO DE LAS IMÁGENES DE PERSONAS MENORES DE EDAD

Cuando se celebren actividades escolares o eventos en centros educativos en los que las personas menores participen, tanto por personas allegadas o familiares como por el propio centro se toman fotografías y se graban vídeos en los que se recogen imágenes de los y las menores.

Si la grabación de las imágenes se produjera por parte del centro escolar con **finés educativos**, como trabajos escolares o evaluaciones, la administración educativa estaría legitimada para hacer dicho tratamiento sin necesidad del consentimiento de los menores o de sus padres/tutores.

Pero cuando la grabación de imágenes no corresponda con dicha función educativa, sino que se trate de imágenes de actividades o eventos que se graban habitualmente con fines de difusión en la revista escolar o en las redes sociales del centro, se necesitará contar con el **consentimiento** de los interesados, a quienes se habrá tenido que informar con anterioridad de la finalidad de la grabación, en especial de si las imágenes van a estar accesibles de manera indiscriminada o limitada a la comunidad escolar o incluso a terceras personas que puedan acceder a su contenido desde plataformas digitales de uso cotidiano.

3.4 LA CESIÓN DE DATOS DE LAS PERSONAS MENORES DE EDAD

Los centros educativos suelen recibir peticiones de otros centros, administraciones y organismos o entidades privadas, para que se les facilite información personal de los y las menores, por ejemplo, de los servicios sociales indicados en el marco legal de esta guía.

La comunicación de datos requiere, con carácter general, el consentimiento de los interesados, de los menores o de sus padres o tutores,

salvo que esté legitimada por otras circunstancias, como que permita u obligue una ley especial, o bien, que se encuentre bajo alguno de los supuesto de excepción señalados por el artículo 8 de la Ley No. 81 del 26 de marzo del 2019 sobre Protección de Datos Personales (*ver anexo 1*), como lo sería atender una urgencia médica, o que se produzca en el marco de una relación jurídica aceptada libremente por ambas partes, por ejemplo, la establecida entre los padres y el centro educativo al matricular a sus hijos.

En estos supuestos se pueden comunicar los datos sin necesidad de obtener el consentimiento de los afectados. En materia de niñez debemos recordar la existencia del principio rector, es decir, el **interés superior del o la menor de edad**. Si bien, el Estado debe aplicarlo como principio general de la actuación administrativa, este principio no es absoluto y tampoco promueve una autorización directa a la administración para ceder los datos de los y las menores de edad en cualquier supuesto.



TUS DATOS PERSONALES



Si una entidad que tiene como actividad la atención social detecta una situación que requiere actuación inmediata sobre una persona menor de edad y no es competente para ello por la especificidad de la atención en estos escenarios, debe comunicar los datos al organismo o entidad competente en materia de atención a la infancia. Sin embargo, esta previsión tiene tres límites:

Sólo se podrá actuar en casos de situaciones en que el o la menor precisa atención inmediata, relacionado claramente con la urgencia;

1.

Solamente se puede poner en conocimiento de un servicio que tenga competencias legales sobre la materia asistencial a la persona menor de edad.

2.

No se habilita a la cesión de expedientes íntegros, sino a la elaboración de informes puntuales, donde se podrán ceder solo aquellos datos estrictamente necesarios para la finalidad perseguida.

3.

4. TRATAMIENTO DE DATOS EN INTERNET

4.1 UTILIZACIÓN DE PLATAFORMAS EDUCATIVAS POR PARTE DE CENTROS DE EDUCACIÓN

Debido al confinamiento durante la pandemia y gracias al veloz desarrollo de las tecnologías de la información, los entes educativos han incrementado el uso de plataformas y tecnologías digitales, tanto para impartir clases, como para colgar y enviar materiales e información de relevancia. En relación a los datos personales, la utilización de plataformas educativas, necesariamente deberá considerar los siguientes aspectos¹:

- Desplegar la diligencia debida para que el encargado del tratamiento garantice el cumplimiento de las medidas de seguridad exigibles.
- Especificar por contrato la naturaleza de los datos para poder definir e implementar las medidas de seguridad adecuadas que deben transmitirse a lo largo de todos los contratos establecidos con los encargados.

¹ Recomendaciones tomadas de las Guías Sectoriales de la Agencia Española de Protección de Datos (AEPD), Guía para Centros Educativos. Disponible en: www.aepd.es/es/documento/guia-centros-educativos.pdf

- Los contratos suscritos deben especificar claramente las responsabilidades de todas las partes intervinientes en la prestación de los servicios de nube, tanto de los centros o Administraciones educativas como de las entidades que actúan como encargadas del tratamiento. Por ejemplo, se deben determinar las responsabilidades sobre las medidas de seguridad que deben implementarse.
- Establecer procedimientos de colaboración entre el responsable y los encargados de tratamiento para la implementación y mantenimiento de las medidas de seguridad, ya que la responsabilidad puede ser, en muchos casos, compartida, por lo que deben delimitarse contractualmente las responsabilidades de cada uno de ellos.
- Los centros educativos deben conocer el procedimiento establecido para la recuperación de los datos en caso de posibles contingencias que puedan producirse.
- El centro educativo debe adoptar las medidas necesarias para que todos los usuarios del sistema sean conocedores de las políticas del centro en materia de seguridad.
- Al finalizar el contrato de prestación de servicios, los centros educativos deben tener la opción de exigir al encargado del tratamiento la portabilidad de la información a sus propios sistemas, o a otro nuevo encargado de tratamiento, con garantías de la integridad de la información. A tal efecto el responsable debe obtener información respecto a la manera de recuperar los datos, de forma que quede garantizada contractualmente la portabilidad.
- Al finalizar la contratación, el encargado del tratamiento tiene que garantizar al responsable del tratamiento el borrado seguro de los datos personales donde se encuentren alojados, de tal forma que se impida su reutilización. Además, deberá asegurar el bloqueo o borrado de todos los usuarios para imposibilitar el acceso a la plataforma educativa. (Se considera una buena práctica que a la finalización del contrato se asegure la destrucción o devolución de los datos con un certificado de destrucción o con un acuse de recibo).

PUBLICACIÓN DE DATOS EN LA WEB Y EN REDES SOCIALES

Podrán publicarse datos relativos a las personas menores en la página web de la institución - como fotografías o vídeos- siempre que se disponga del consentimiento de sus padres o tutores. También podría llevarse a cabo de manera que no se pudiera identificar a los menores, **por ejemplo:** pixelando las

imágenes o tomando la fotografía de espaldas, de manera que no sean identificables.

Además, sería posible su publicación cuando responda a determinados eventos desarrollados en el entorno escolar con la única finalidad de que los padres pudieran tener acceso a ella. Este acceso deberá llevarse a cabo siempre en un entorno seguro que exigiera la previa identificación y autenticación de los menores, padres o tutores (**por ejemplo:** en un área restringida de la intranet del centro), limitándose a la información correspondiente a eventos en los que el menor hubiera participado.

En el caso de que la página web, sea de contenido abierto y se incluyeran datos que permitieran la identificación de los menores, se requeriría su consentimiento o el de sus padres o tutores. En estos supuestos se recomienda **disociar o anonimizar** los datos de los menores, de manera que no se les pueda identificar.

5. EJERCICIO DE LOS DERECHOS ARCO

5.1 ¿QUÉ PROCESO DEBEMOS SEGUIR PARA GARANTIZAR EL EJERCICIO LOS DERECHOS ARCO? ACCESO, RECTIFICACIÓN, CANCELACIÓN, OPOSICIÓN Y PORTABILIDAD

Para el ejercicio de un derecho ARCO (derechos de acceso, rectificación, cancelación, oposición y portabilidad) por parte de personas menores o bien, sus padres o tutores, se debe contar con un protocolo de actuación que establezca todos los pasos a seguir desde la recepción de la solicitud hasta la notificación de la resolución.

El primer paso que ha de seguir el personal que reciba una solicitud de ejercicio de un derecho ARCO es saber a qué departamento o persona del servicio se debe remitir la solicitud. Se debe tomar en cuenta que ejercicio de estos derechos ARCO es **personalísimo**, por lo que sólo podrá solicitarlo la persona interesada, en el caso específico de menores, serán sus padres o tutores legales.

Dada la complejidad o el tiempo que requiere el análisis de la solicitud frente a la brevedad de los plazos de resolución de acuerdo al artículo 16 de la Ley No. 81 de 26 de marzo de 2019, sobre Protección de Datos Personales (No mayor de 10 días hábiles a partir de la fecha de presentación de dicha

solicitud). Las instituciones podrán facilitar el acceso ciudadano a través de formularios colgados en una página web y designar a una persona encargada de la atención de derechos ARCO.



5.2 ¿CÓMO PROCEDER CUANDO SE RECIBE UNA PETICIÓN?



Cuando en el servicio de atención a derechos ARCO establecido se reciba una petición, se deberá poner sello o firma y fecha de recepción, para tener constancia del plazo para la contestación y remitirá la solicitud al personal competente para su tramitación y resolución que, recibida la solicitud, verificará si cumple con los requisitos mínimos:

1. Nombre y apellidos de la persona interesada.
2. Fotocopia de su cédula de identidad personal o pasaporte. Si la solicitud se realiza por medios telemáticos será válida la firma electrónica identificativa.
3. Dirección para notificaciones.
4. Fecha y firma de la solicitud.
5. Contenido de la solicitud.

Una vez obtenida esta información, el personal de atención de derechos ARCO enviará a la persona solicitante la información a través de correo certificado u otra forma de comunicación que permita dejar constancia de su recepción como el correo electrónico, siendo responsable de conservar la documentación que soporta el proceso.

5.3 ¿CUÁL ES EL CONTENIDO DE LA INFORMACIÓN QUE EL RESPONSABLE DE LOS DATOS DEBERÁ PROPORCIONAR AL TITULAR?

Además, se deberá contemplar lo establecido en los artículos 14 y 15 del Reglamento a la Ley de Protección de Datos, Decreto Ejecutivo No. 285 del 28 de mayo del 2021, en cuanto al contenido de la información que el responsable de los datos deberá proporcionar al titular, sea:

1. La identidad y datos de contacto del responsable del tratamiento.
2. La finalidad o finalidades del tratamiento a que se destinarán los datos personales; cuando el responsable del tratamiento proyecte el tratamiento posterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento posterior, información sobre ese otro fin y cualquier

información adicional pertinente.

3. La condición que legitima el tratamiento conforme a los artículos 6, 8, 33 de la Ley 81 del 26 de marzo del 2019. Cuando el tratamiento esté basado en el consentimiento del interesado, se le debe informar de su derecho a revocar el consentimiento en cualquier momento, sin que ello tenga efectos retroactivos; cuando el tratamiento de datos personales sea un requisito legal o un requisito necesario para suscribir un contrato, así se indicará y cuando el tratamiento se base en los intereses legítimos del responsable del tratamiento o de un tercero, conforme al artículo 8 de la Ley 81 de del 26 de 2019 , se detallará cuáles son estos intereses.
4. Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.
5. La intención del responsable del tratamiento de transferir datos personales a un tercer país, así como la condición prevista en el artículo 33 de la Ley 81 del 2019 que resulta aplicable.
6. El plazo durante el cual se conservación de los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.
7. La existencia, forma y de mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad.
8. La existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 19 de la Ley 81 de 2019 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.
Los datos de contacto del oficial de datos personales.
9. Cuando los datos personales no se hayan obtenido de su titular, el responsable del tratamiento le facilitará, además de la información a que se refiere este artículo, la referente a la categoría de los datos de que se trate y la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.

6. GLOSARIO

Almacenamiento de datos. Conservación o custodia de datos en una base de datos establecida en cualquier medio provisto, incluido el de las tecnologías de la información y la comunicación (TICs).

Autoridad de control. La autoridad Nacional de Transparencia y Acceso a la Información (ANTAI), es el organismo de la administración pública responsable de supervisar, implementar y controlar el cumplimiento de la Ley 81 de 2019 y el presente decreto, en todo el territorio nacional.

Base de datos. Conjunto ordenado de datos de cualquier naturaleza, cualquiera que sea la forma o modalidad de su creación, organización o almacenamiento, que permite relacionar los datos entre sí, así como realizar cualquier tipo de tratamiento o transmisión de estos por parte de su Custodio.

Bloqueo de datos. Restricción temporal de cualquier acceso o tratamiento de los datos almacenados.

Consentimiento. Manifestación de la voluntad del titular de los datos, mediante la cual se efectúa el tratamiento de estos.

Dato anónimo. Aquel dato cuya identidad no puede ser establecida por medios razonables o el nexo entre este y la persona natural a la que se refiere. Datos biométricos. Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona natural que permitan o confirmen la identificación única de dicha persona.

Dato caduco. Aquel dato que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado por su vigencia o si no hubiera Norma expresa, por el cambio de los hechos o circunstancias que Consigna.

Datos confidenciales. Aquellos datos que por su naturaleza no deben ser de conocimiento público o de terceros no autorizados, incluyendo aquellos que estén protegidos por la ley, por acuerdos de confidencialidad o no divulgación, afín de salvaguardar información. En los casos de la Administración pública, son aquellos datos cuyo tratamiento está limitado para fines de esta administración o si se cuenta con el conocimiento expreso del titular, sin perjuicio de lo dispuesto por las leyes especiales o por las normativas que las desarrollen. Los datos confidenciales siempre serán de acceso restringido.

Dato disociado. Aquel dato que no puede asociarse al titular ni permitir por su estructura, contenido o grado de desagregación la identificación de la persona, sea está natural.

Datos genéticos. Datos personales relativos a las características genéticas heredadas o adquiridas de una persona natural que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

Dato personal. Cualquier información concerniente a personas naturales, que la identifica o las hace identificables.

Datos relativos de la salud. Datos personales relativos a la condición física o mental de una persona natural, que revelan información sobre su estado de salud.

Dato sensible. Aquel que se refiera a la Esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. De manera enunciativa cómo se consideran sensible los datos personales que puedan relevar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, a la preferencia u orientación sexual, datos genéticos o datos biométricos, entre otros, sujetos a regulación y dirigidos a identificar de manera unívoca a una persona natural.

Derechos ARCO. Derechos irrenunciables básicos de los titulares de datos personales, e identificarlos como: derechos de acceso, rectificación, cancelación y oposición.

Destinatario. La persona natural o jurídica, autoridad pública, servicio u organismo al que se transfieran datos personales.

Elaboración de los perfiles. Toda forma de tratamiento automatizado que utilice datos personales para evaluar determinados aspectos de una persona natural y en particular para analizar o predecir aspectos relativos a su rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos.

Eliminación o cancelación de datos. Suprimir o borrar de forma permanente los datos almacenados en las bases de datos, cualquiera que sea el procedimiento empleado para ello.

Exportador. Persona natural o jurídica de carácter público o privado, domiciliado en el país, que efectúe transferencias de datos personales extrafronterizos, conforme a lo dispuesto en la Ley 81 de 2019 y el presente

decreto.

Evaluación de impacto en protección de datos. Documentación del responsable del tratamiento que contiene la descripción de los procesos con datos personales que pueden generar riesgos para los derechos y deberes individuales y sociales, así como medidas, salvaguardas y mecanismo de migración de riesgo.

Ficha técnica. Documento que contiene los registros, protocolos y las reglas, relacionados al almacenamiento y tratamiento de los datos personales.

Fuente de accesible. Bases de datos que no sean de acceso restringido o contengan reserva alguna a consultas, o que sean de acceso público, cómo las publicaciones estatales de carácter oficial, los medios de comunicación, los directorios telefónicos y la lista de personas que pertenecen a un grupo de profesionales que contengan únicamente nombre, título o profesión, actividad, dirección laboral o comercial, al igual que información que indique su pertenencia a organismos.

Oficial de protección de datos personales. Funcionario designado para atender.

Modificación de datos. Toca en el contenido de los datos almacenados en base de datos.

Procedimiento de disociación o anonimizarían. Todo tratamiento de datos que impide que la información disponible en la base de datos puede asociarse a persona natural determinada o determinable.

Regulador. Entidad del estado del estado encargada de fiscalizar a los sujetos de sectores lados por las leyes especiales.

Responsable del tratamiento de los datos. Persona natural o jurídica, de derecho público o privado, lucrativa o no, qué le corresponde las decisiones relacionadas con el tratamiento de los datos y que determina los fines, medios y alcance, así como cuestiones relacionadas a estos.

Titular de los datos. Persona natural a la que se refiere los datos.

Transferencia de datos. Dar a conocer, divulgar, comunicar, intercambiar y/o transmitir, de cualquier forma y por cualquier medio, de un punto a otro, intra o extra fronterizo, los datos a personas naturales o jurídicas distintas del titular, ya sean determinadas o indeterminadas.

Tratamiento de datos. Cualquier operación o complejo de operaciones o procedimientos técnicos como de carácter automatizado o no, que permite 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. Son ejemplos de tratamiento:

- La obtención de nuevos datos a partir de la información recabada
- La actualización de la información existente en una base de datos a partir de los nuevos datos recabados.
- La eliminación de los datos existentes en una base de datos
- La simple consulta de datos de una base de datos
- Facilitar el acceso a los datos de una persona física por parte de una tercera persona física o jurídica, mediante cualquier tipo de comunicación, consulta, interconexión o transferencia.

Violación de la seguridad de los datos personales. Toda infracción a la seguridad que ocasioné la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

7. BIBLIOGRAFÍA

O.N.U. Convención sobre los Derechos del Niño. <https://www.un.org/es/events/childrenday/pdf/derechos.pdf>

O.N.U. Declaración Universal de Derechos Humanos. <https://www.un.org/es/about-us/universal-declaration-of-human-rights>

Constitución Política de la República de Panamá, Gaceta Oficial https://www.organojudicial.gob.pa/uploads/wp_repo/blogs.dir/cendoj/CONSTITUCIONES_POLITICAS/constitucion_politica.pdf

Ley No. 81 de 26 de marzo de 2019, sobre Protección de Datos Personales https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf

Reglamento a la Ley de Protección de Datos. Decreto Ejecutivo No. 285 del 28 de mayo de 2021 <https://www.antai.gob.pa/reglamentacion-de-la-ley-n-81-de-proteccion-de-datos-personales/>

Estándares Iberoamericanos de Protección de Datos Personales aprobados en el 2017: <https://www.redipd.org/es/documentos/estandares-iberoamericanos>

Ley No. 47 de 1946, Ley Orgánica de Educación https://www.meduca.gob.pa/sites/default/files/2016-01/1946_ley_00047_25042_2004.pdf

Ley No. 148 de 21 de abril de 2020, que crea el Programa de Asistencia Social Educativa Universal https://www.asamblea.gob.pa/APPS/SEG_LEGIS/PDF_SEG/PDF_SEG_2020/PDF_SEG_2022/2022_A_187.pdf

Ley No 171 del 15 de octubre de 2020) de Protección Integral a la Primera Infancia y al Desarrollo Infantil Temprano https://www.gacetaoficial.gob.pa/pdfTemp/29135_C/GacetaNo_29135c_20201015.pdf

Red Iberoamericana de Protección de Datos. Informe 2016 Tema monográfico: la protección de datos de los menores de edad. www.redipd.org/sites/default/files/inline-files/Primer_informe_Red_Iberoamericana_de_Proteccion_de_Datos.pdf

Guías Sectoriales de la Agencia Española de Protección de Datos (AEPD), Guía para Centros Educativos. Disponible en: www.aepd.es/es/documento/guia-centros-educativos.pdf

8. ANEXOS

1. EXCEPCIONES QUE LEGITIMAN EL TRATAMIENTO DE DATOS PERSONALES

1. Se deben contemplar las excepciones en el artículo 8 de la Ley no. 81 del 26 de marzo del 2019, mismas que podrían autorizar el tratamiento de datos personales, en los siguientes casos:
2. Datos que provengan o que se recolecten de fuentes de dominio público o accesible en medios públicos.
3. Los que se recolecten dentro del ejercicio de las funciones propias de la Administración Pública en el ámbito de sus competencias.
4. Los de carácter económico, financiero, bancario o comercial que cuenten con el consentimiento previo.
5. Los que se contengan en listas relativas a una categoría de personas que se limiten a indicar antecedentes, como la pertenencia de la persona natural a una organización, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento.
6. Los que son necesarios dentro de una relación comercial establecida, ya sea para la atención directa, comercialización o venta de bienes o servicios pactados.
7. El tratamiento de datos personales que realicen organizaciones privadas para el uso exclusivo de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquellos.
8. Los casos de urgencia médica o sanitaria.
9. El tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
10. El tratamiento que sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o para un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un menor de edad o una persona con discapacidad.

2. PROTOCOLOS DE NOTIFICACIÓN Y DOCUMENTACIÓN EN CASO DE SUFRIR VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

En atención a los artículos 37 y 38 del Decreto Ejecutivo No. 285 de 28 de mayo de 2021, Reglamento de la Ley 81 de marzo del 2019, sobre protección de datos personales, cuando el responsable del tratamiento tenga conocimiento de una vulneración de seguridad, entendida esta como cualquier daño, pérdida, alteración, destrucción, acceso y en general, cualquier uso ilícito o no autorizado de los datos personales, aun cuando ocurra de manera accidental, en cualquier fase del tratamiento y que represente un riesgo para la protección de los datos personales, notificará de inmediato dicho incidente a la autoridad de control y a los titulares afectados.

El custodio de la base de datos deberá informar al responsable del tratamiento de manera inmediata cuando tenga conocimiento de una violación de seguridad.

La notificación que realice el responsable del tratamiento a los titulares afectados estará redactada en un lenguaje claro y sencillo.

La notificación se realizará en el plazo de las 72 y horas a partir de que se conozca el incidente y contendrá, al menos, la siguiente información:

- 1.** La naturaleza del incidente
- 2.** Los datos personales comprometidos.
- 3.** Las acciones correctivas realizadas de forma inmediata
- 4.** Las recomendaciones al titular sobre las medidas que este pueda adoptar para proteger sus intereses
- 5.** Los medios disponibles al titular para obtener mayor información al respecto.

Documentación de las violaciones de la seguridad de los datos personales

El responsable del tratamiento documentará toda violación de seguridad de los datos personales ocurrida en cualquier fase del tratamiento, identificando, como mínimo, la siguiente información y conservándola a disposición de la autoridad de control:

1. La fecha en que ocurrió
2. El motivo de la violación
3. Los hechos relacionados con ella y sus efectos
4. Las medidas correctivas implementadas de forma inmediata y definitiva.

La autoridad de control verificará la gravedad del incidente y para salvaguardar los derechos de los titulares, podrá ordenar que el responsable del tratamiento adopte medidas, tales como la amplia difusión del hecho en los medios de comunicación y/o medidas para revertir o mitigar los efectos del incidente.

Cuando la violación de seguridad tenga lugar en redes públicas de comunicación, se atenderá también con la seguridad pública y la defensa nacional.



Síguenos en nuestras redes **sociales**



@antaipma



@antaipanama



@ANTAI_Panama

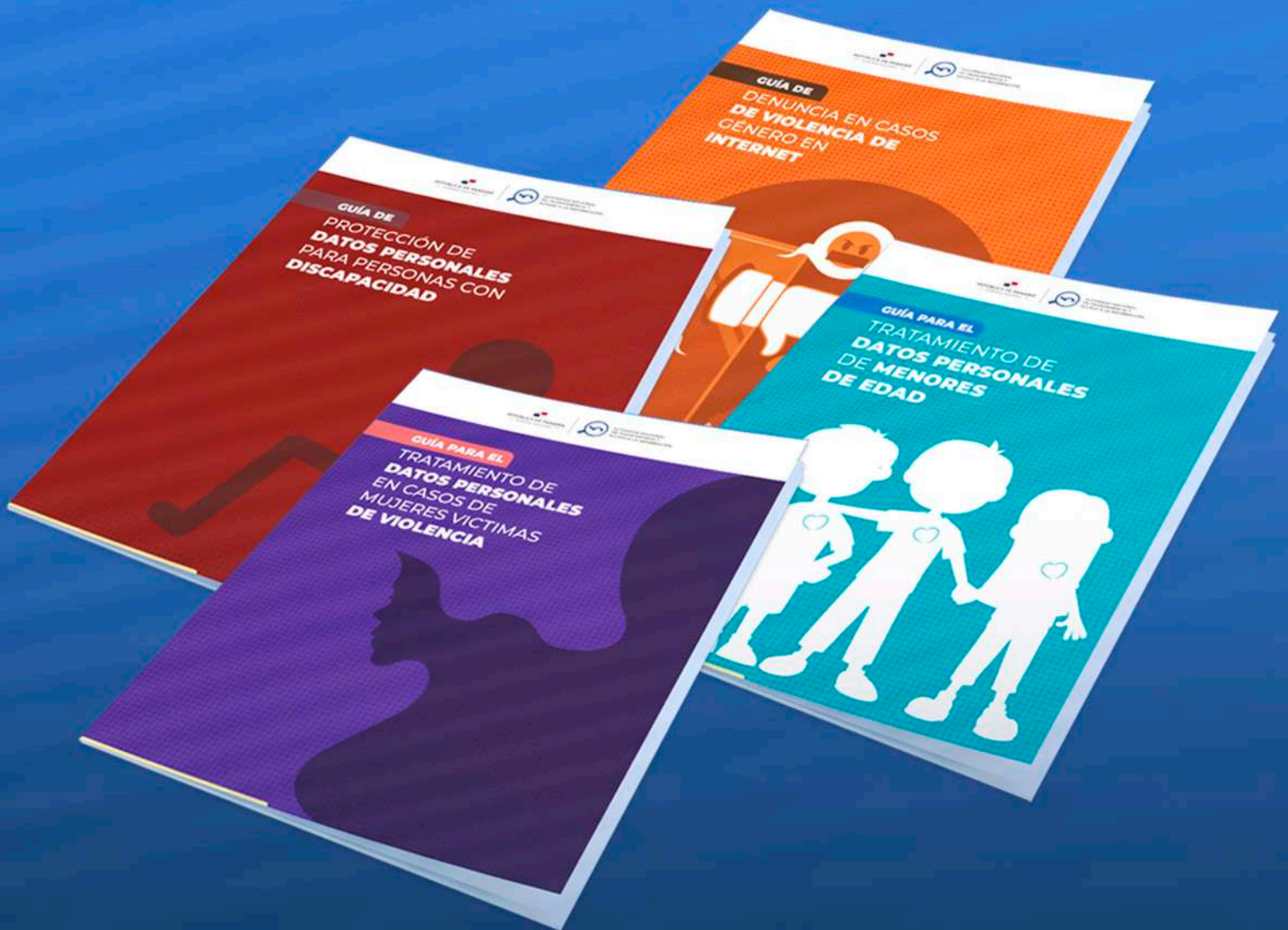


ANTAI PANAMÁ

#PorUnPanamáTransparente

GUÍAS DISPONIBLES EN

 www.antai.gob.pa





GOBIERNO NACIONAL
★ CON PASO FIRME ★



ANTAI

AUTORIDAD NACIONAL
DE TRANSPARENCIA Y
ACCESO A LA INFORMACIÓN


REPÚBLICA DE PANAMÁ
— GOBIERNO NACIONAL —

AUTORIDAD NACIONAL
DE TRANSPARENCIA Y
ACCESO A LA INFORMACIÓN

 www.antai.gob.pa