REPÚBLICA DE PANAMÁ
GOBIERNO NACIONAL

AUTORIDAD NACIONAL
DE TRANSPARENCIA Y
ACCESO A LA INFORMACIÓN

GUÍA PARA EL TRATAMIENTO DE **DATOS PERSONALES** EN CASOS DE MUJERES VICTIMAS **DE VIOLENCIA**

ÍNDICE

PRESENTACIÓN

La Corte Interamericana de Derechos Humanos (CIDH) observa que el derecho de las mujeres a vivir libres de violencia y discriminación, ha sido consagrado y establecido como un desafío prioritario en los sistemas de protección de los derechos humanos a nivel regional e internacional, lo que requiere una actuación coordinada y eficaz entre los distintos servicios que prestan atención a las mujeres que sufren violencia.

Según estadísticas del Ministerio Público de Panamá[1], los casos de violencia doméstica aumentaron 13% en el primer trimestre del presente año. Las cifras indican que entre enero y marzo de 2022 hubo 4.799 denuncias, 629 más que en el mismo periodo del año pasado. Por lo que, en Panamá, cada 30 minutos se registra un acto de violencia doméstica.

El concepto de "acceso a la justicia" de conformidad con los parámetros internacionales de derechos humanos, ha establecido que un acceso adecuado a la justicia no se circunscribe solamente a la existencia formal de recursos judiciales y administrativos, sino también a que éstos sean idóneos para prevenir, investigar, sancionar y reparar las violaciones denunciadas.

Por esta razón, la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI), pone a disposición la presente guía que permitirá mejorar la coordinación interinstitucional en el tratamiento de los datos personales de las mujeres víctimas de violencia con el objetivo de garantizar la privacidad de quienes acuden a las instituciones y con ello, la protección de otros derechos fundamentales como el derecho a la intimidad, la libertad de expresión y a vivir una vida digna y libre de violencia.

Esta guía pretende orientar mediante algunos ejemplos que no son exhaustivos sobre el deber de coordinación entre organismos, entes y departamentos competentes para ofrecer respuestas que faciliten el proceso de atención y garanticen a las mujeres el control de los datos sobre su persona. Así, se busca fomentar la coordinación ordenada y eficiente, garantizando el respeto a la protección de los datos de las mujeres que sufren de violencia.

1 Informes Estadísticos Violencia Doméstica disponibles en la página web del Ministerio Público de Panamá: https://ministeriopublico.gob.pa/estadisticas-judiciales/violencia-domestica/

OBJETIVOS

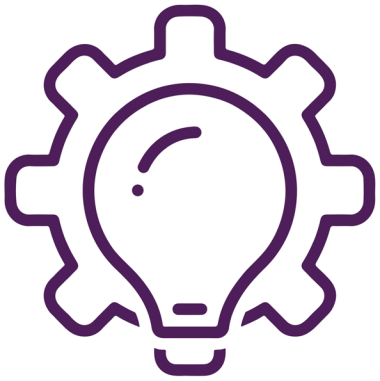
OBJETIVO GENERAL

- El objetivo de la presente guía es brindar un marco procedimental para las personas encargadas de prevenir, atender e investigar casos de mujeres víctimas de violencia con pleno respeto a la protección de datos personales.

OBJETIVOS ESPECÍFICO

- Promover el conocimiento con respecto a la Ley No. 81 del 26 de marzo de 2019, sobre protección de datos personales.
- Ofrecer información a las instituciones públicas encargadas de atender, prevenir, investigar, sancionar y atender los casos de mujeres víctimas de violencia, que les permita hacer un uso y tratamiento adecuado y eficiente de los datos persónales, acuerdo a las disposiciones de la Ley No. 81 del 26 de marzo de 2019, sobre protección de datos personales y su respectivo decreto.
- Brindar un marco de referencia que permita a las instituciones competentes en la materia estrechar su coordinación para asegurar una respuesta oportuna a las demandas de las mujeres que luchan para acceder al derecho fundamental a una vida libre de violencia.

METODOLOGÍA



La presente guía se basa en investigación bibliográfica, documental e información obtenida y facilitada por instituciones competentes de atender la violencia contra las mujeres. Los datos cualitativos se han obtenido en un período de cuatro semanas entre octubre y noviembre, mediante recopilación de información obtenida de repositorios públicos, páginas oficiales de las instituciones públicas y entrevistas a personas funcionarias públicas en instituciones clave en el tema.

Las solicitudes de entrevistas fueron dirigidas a personas funcionarias públicas que trabajan en instituciones claves para atender los caso de mujeres víctimas de violencia en Panamá. Así, se obtuvo una entrevista con la Dirección de Derechos Humanos del Instituto Nacional de la Mujer (INAMU), cuya información fue de gran utilidad pues el INAMU funciona como ente rector del Comité Nacional contra la Violencia en la Mujer (CONVIMU), fuente que proporcionó información de alta relevancia para diseñar la presente guía.

En el caso de la entrevista, su duración fue de aproximadamente 30 minutos y fue realizada mediante plataformas digitales y por medio de un cuestionario por escrito remitido mediante correo electrónico. El guion de la entrevista se estructuró en seis preguntas, algunas de ellas con sub preguntas a desarrollar, todas las preguntas eran abiertas.

Por otro lado, también fue posible obtener información relevante aportada por la Procuraduría General de la Nación (Fiscalía de la República de Panamá) a través del formulario de entrevista remitido y contestado vía correo electrónico.

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 con antelación.

MARCO LEGAL

A) LEGISLACIÓN APLICABLE

Panamá posee un marco legal robusto para proteger el derecho fundamental a la protección de datos personales con enfoque de género, teniendo como antecedentes la Ley N.° 17 del 26 de marzo del 2001, por medio de la cual se aprueba el protocolo facultativo de la Convención sobre la Eliminación de todas las Formas de Discriminación Contra la Mujer, adoptado por la Asamblea General de las Naciones Unidas en fecha 6 de octubre de 1999.

Por otro lado, el país se encuentra adherido a la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la mujer (Convención de Belén do Pará) del 24 de abril de 1995; y tras haber aprobado leyes específicas como la Ley N.° 82 del 24 de octubre del 2013 que adopta medidas de prevención contra la violencia en las mujeres y su respectiva reforma al Código Penal es posible tipificar el femicidio y sancionar los hechos de violencia contra la mujer.

Aunado a ello, la Constitución Política de la República de Panamá regula el tema de protección de datos personales mediante su numeral 42, que indica: “Toda persona tiene derecho a acceder a la información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la Ley. Esta información sólo podrá ser recogida para fines específicos, mediante consentimiento de su titular o por disposición de autoridad competente con fundamento en lo previsto en la Ley”.

En lo específico, Panamá cuenta con la Ley No. 81 del 26 de marzo de 2019, sobre protección de datos personales y su respectivo reglamento, emitido mediante Decreto Ejecutivo No. 285 del 28 de mayo de 2021, normas que establecen lineamientos obligatorios para la Protección de Datos Personales bajo una ley de vanguardia en la región que, articulada con las normas previamente citadas y otros instrumentos concordantes, permite generar una vinculación normativa para atender de manera efectiva y coordinada el tratamiento de datos personales en relación al flagelo de la violencia de género contra las mujeres.

La presente guía ha tenido como referencia esta legislación vigente en materia de lucha contra la violencia de género y protección de datos personales aplicable al

tratamiento de la información personal de las mujeres víctimas de violencia a que se hace referencia y, además las siguientes normas:

- Declaración Universal de los Derechos Humanos de 10 de diciembre de 1948.
- Estándares Iberoamericanos de Protección de Datos Personales aprobados en el 2017.

B) SISTEMA DE COORDINACIÓN INSTITUCIONAL

El objetivo de la presente guía es brindar un marco procedimental para la institucionalidad encargada de atender e investigar casos de mujeres víctimas de violencia con pleno respeto a la protección de datos personales.

La normativa de protección de datos es una herramienta que contribuye a proteger la seguridad de las mujeres y resguardar sus derechos para evitar que, a los antecedentes producidos por el daño físico, psicológico, social o económico experimentado por las víctimas de violencia, se agregue una segunda victimización derivada de un inadecuado tratamiento de su información personal en la ejecución de los procesos administrativos y judiciales.

Como respuesta institucional al problema de la violencia contra las mujeres se han establecido en Panamá, mecanismos necesarios para la mejora de la coordinación entre las instituciones implicadas en la asistencia a las mujeres víctimas de maltrato y de violencia. A continuación, se describen los principales mecanismos de coordinación interinstitucional, los cuales se recomienda incluir en sesiones de trabajo y talleres de sensibilización sobre la aplicación de la presente guía:

I. Comité Nacional contra la Violencia en la Mujer (CONVIMU)

El Comité Nacional contra la Violencia en la Mujer (CONVIMU) fue creado por la Ley No. 82 de 2013, que como se mencionó anteriormente, tipifica el femicidio y sanciona la violencia contra la mujer, entre otros aspectos.

Este Comité está conformado por 15 instituciones públicas, y también por representantes de organizaciones de la sociedad civil con trayectoria comprobable en la lucha contra la violencia hacia las mujeres. El CONVIMU responde al Instituto Nacional de la Mujer (INAMU), y dentro de sus funciones se encuentran: diseñar políticas para prevenir y erradicar la violencia contra las mujeres; monitorear las políticas existentes

para tal fin; vigilar que los medios de comunicación no fomenten la violencia contra las mujeres y que organizaciones de la sociedad civil fomenten el ingreso y la participación igualitaria de mujeres sin discriminación alguna; así como apoyar técnicamente al Instituto Nacional de la Mujer para vigilar el cumplimiento de la Ley 82 y monitorear la situación de violencia contra las mujeres en el país.

II. Observatorio Panameño contra la Violencia de Género (OPVG)

Por otro lado, existe el Observatorio Panameño contra la Violencia de Género (OPVG), que es un organismo interinstitucional, creado mediante convenio en el año 2009. El OPV es coordinado por la Defensoría del Pueblo de la República de Panamá y está integrado por entidades públicas y representantes de la sociedad civil.

Las entidades públicas que lo conforman son:

- El Órgano Judicial
- La Procuraduría General de la Nación
- El Ministerio de Seguridad Pública
- El Ministerio de Gobierno
- El Ministerio de Desarrollo Social
- El Ministerio de Salud
- El Ministerio de Educación
- El Ministerio de Trabajo y Desarrollo Laboral
- El Ministerio de Economía y Finanzas
- El Instituto Nacional de la Mujer
- La Caja de Seguro Social
- El Instituto de la Mujer de la Universidad de Panamá
- La Defensoría del Pueblo
- La Contraloría General de la República de Panamá

Otras entidades, Organizaciones Públicas y Privadas son:

- El Colegio Nacional de Abogados
- El Consejo Nacional de Periodismo
- La Fundación de Asistencia Legal Comunitaria

Organizaciones No Gubernamentales de Mujeres (ONGs) con representación a nivel nacional en la lucha contra la violencia de género:

- Voces Vitales
- Centro de la Mujer Panameña
- Alianza del Movimiento de Mujeres
- Centro para el Desarrollo de la Mujer
- Espacio de Encuentro de Mujeres
- Centro de Estudios y Capacitación Familiar
- Fundación para la Equidad de Género
- Asociación de Magistradas y Juezas de Panamá
- Coordinadora Nacional de Mujeres Indígenas de Panamá
- Comité de América Latina y El Caribe para la Defensa de los Derechos de las Mujeres

Las funciones del Observatorio Panameño contra la Violencia de Género (OPVG) son las siguientes: colaborar en la recolección, análisis y difusión de información periódica homogénea y sistemática relativa a la violencia de género en Panamá; Apoyar en la modernización y actualización de sistemas de información, y crear otras bases de datos que sirvan de referencia para dar seguimiento a la situación de violencia de género en Panamá; Servir de organismo de consulta y colaborar en el diseño de propuestas de actuación, en distintos ámbitos, tendientes a prevenir, sancionar y erradicar la violencia de género y a mejorar la situación de las mujeres víctimas de la misma; Velar por el cumplimiento de la normativa nacional e internacional, de la efectividad de los planes, políticas y programas dirigidos a la erradicación del fenómeno de la violencia de género; y **promover alianzas, pactos, acuerdos, protocolos de actuación entre las instituciones involucradas con el tratamiento de la violencia de género en Panamá.**

Por otro lado, también se encargan de estudiar la legislación existente sobre el tema y la legislación general desde una perspectiva de género; Analizar las decisiones judiciales en torno al problema de la violencia de género; Diseñar y promover acciones de investigación multidisciplinaria destinadas a comprender mejor el fenómeno de la violencia de género; Promover campañas de sensibilización en materia de equidad de género; Servir de foro de encuentro e intercambio de opiniones en esta materia; Fomentar y estimular el mejoramiento técnico y social de las instancias involucradas en la atención de las víctimas de violencia de género; y documentar las medidas y actuaciones puestas en marcha por las administraciones públicas, así como por entidades privadas, para prevenir, detectar y erradicar la violencia de género.

III. Consejo de Protección de Datos Personales

La Ley No. 81 de 26 de marzo de 2019, crea el Consejo de Protección de Datos Personales que tiene como funciones: asesorar a la ANTAI en relación con la Ley, recomendar políticas públicas, evaluar casos presentados para consultas y desarrollar un reglamento interno. **Dicho órgano estará conformado por:**

El Ministro del Ministerio de Comercio e Industria	El Administrador General de la Autoridad de Protección al Consumidor y Defensa de la Competencia (ACODECO)
El Director General de la ANTAI	El Defensor del Pueblo, o quien éste designe
Un representante del Consejo Nacional de la Empresa Privada (CONEP)	Un representante del Colegio Nacional de Abogados
Un representante de la Asociación Bancaria de Panamá	Un representante del Tribunal Electoral
Un representante de la Cámara de Comercio, Industria y Agricultura de Panamá	

En el marco de este sistema de articulación interinstitucional resulta pertinente la socialización de la presente guía con la finalidad de mejorar la coordinación y con ello la eficacia en las acciones realizadas a partir de recursos públicos.

Los esquemas anteriormente presentados permiten generar sinergias entre las instituciones de manera que puedan estrechar coordinaciones y actualizar sus protocolos a los tiempos que vivimos, es por ello que se insta a promover también, la **firma de convenios de cooperación interinstitucional** a fin de generar campañas de comunicación y sensibilización conjunta en materia de protección de datos personales para mujeres victimas de violencia y ciber violencias o violencias mediáticas.

1. GUÍA DE TRATAMIENTO DE DATOS PERSONALES

PROCESOS DE MUJERES VÍCTIMAS DE VIOLENCIA

Cuando una mujer víctima de violencia se acerca a un servicio de atención o asesoramiento se debe informar de modo expreso y preciso, lo siguiente:

A. La identificación de la propia institución que obtiene/recaba los datos personales. En tanto que no se puede dar por un hecho que todas las víctimas al momento de recibir la atención primaria, se encuentren conscientes frente a quién se encuentran.

B. Los datos personales o las categorías de datos que se le van a solicitar, de modo que haya información clara y certeza al respecto.

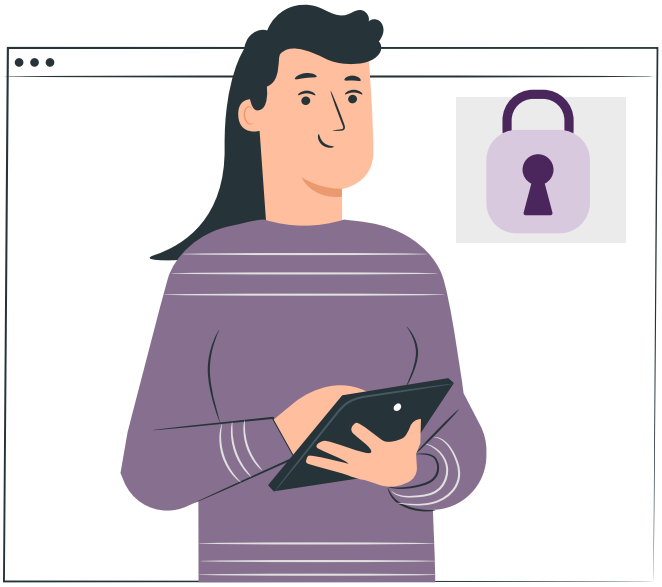
C. Que los datos facilitados serán incorporados a una base de datos (indicar cual) y se informará de forma transparente y puntual las finalidades del tratamiento. Ello con el objetivo de brindar certeza sobre el manejo que se dará a esos datos.

D. Que tiene el deber de suministrar datos reales que le sean solicitados, así como el de colaborar en su obtención, especialmente cuando sean necesarios con motivo de la asistencia por razones de interés público.

E. De la posibilidad de ejercer los derechos ARCO- de acceso, rectificación, cancelación y oposición y portabilidad- en las condiciones legalmente establecidas. Así como la identidad y dirección de la organización, entidad o servicio responsable de la base de datos, en su caso, de su representante, ante el cual puede ejercitar los referidos derechos de acceso, rectificación, cancelación, oposición y portabilidad. En este sentido se debe informar a la víctima sobre los **mecanismos** a través de los cuales puede ejercer sus derechos (al menos el sitio o lugar donde se puede consultar esa información).

F. Es importante informarle que los datos que se entreguen serán confidenciales y sólo serán tratados por personas autorizadas y que tengan una relación con la finalidad para la cual fue recopilada su información.

G. Debe también informar si existe la intención de realizar cesiones o transferencias de estos datos a otras administraciones públicas, personas u organizaciones privadas -la persona debe ser informada de este aspecto en el momento de la recopilación de los datos, y debe dársele la opción de dar su consentimiento para ello o no darlo. En este sentido sería valioso que se le informe a la víctima a quién se le podrían estar transfiriendo los datos y la finalidad de esa transferencia.



Por ejemplo: Si en relación a la problemática de violencia denunciada la persona requiere un subsidio o apoyo económico del Estado, sus datos podrían ser transferidos al Ministerio de Desarrollo Social (MIDES). En este sentido la víctima deberá ser debidamente informada sobre las autoridades a quienes se les transfieran los datos y las razones de esa transferencia. Esta transferencia deberá darse a la luz del principio de minimización de datos, es decir, aplicar medidas técnicas y organizativas para garantizar que sean objeto de tratamiento los datos que únicamente sean necesarios y precisos para cada uno de los fines específicos del tratamiento.

1.2. ¿QUÉ DEBEMOS OBSERVAR A LA HORA DE RECOPILAR DATOS?

CONFIDENCIALIDAD EN LA RECOPILACIÓN

A. No se deben recoger datos personales de mujeres víctimas de violencia en salas comunes, salas compartidas con personal dedicado a otras cuestiones, o lugares que no permiten el debido aislamiento acústico. Las administraciones deben realizar un esfuerzo de adaptación física y lógica para cumplir con este objetivo.

B. Tampoco debe señalarse con carteles una zona para la atención a este colectivo que permita la identificación visual de aquellas personas que necesitan esta ayuda, ni la ubicación de listas que identifiquen a las mujeres víctimas de violencia, **por ejemplo**, con una serie de citas horarias o similares.

C. Si existe riesgo de no localizar adecuadamente los puntos de atención institucional, debe procurarse generar una ventanilla informativa a la entrada que relacione los departamentos con la actividad que desarrolla. **Por ejemplo: Sala 1- violencia contra las mujeres** y que dicho departamento se identifique con un número de referencia dado a la persona, no con nombres u otros datos que la puedan identificar. Otra posibilidad es que el servicio de información -preferiblemente ubicado a la entrada de las oficinas- acompañe y oriente a las personas interesadas.

D. En este sentido lo más importante es **evitar procesos de revictimización**, por lo que se trata de impedir que terceras personas puedan identificar a las víctimas como tales. Por lo que, una vez iniciada la recopilación de información, ésta se debe realizar **en lugares cerrados con acceso restringido y proporcionando la debida intimidad.**

CALIDAD DE LA INFORMACIÓN A RECOPILAR

A. Hay que señalar que la aplicación estricta de los principios de lealtad, veracidad y exactitud previstos en la Ley No. 81 del 26 de marzo del 2019, sobre Protección de Datos Personales, exige la recopilación de aquellos datos que sean proporcionales. pertinentes y, sobre todo, no excesivos para la finalidad para la que se recogen.

B. En principio, la posibilidad de recoger datos de terceras personas (familiares o personas conocedoras de los hechos, o incluso el propio agresor) debe restringirse al máximo, recogiendo solo los datos estrictamente necesarios y con la indicación de tratarse de datos referidos - esto es, relativos a terceras personas- y respecto de los cuales no consta el consentimiento para la recopilación.

C. Respecto a los hijos e hijas menores de edad, no sería preciso adoptar ninguna medida, ya que el consentimiento lo suple la voluntad de alguno de los progenitores. Sin embargo, tratándose de hijos o de hijas mayores de edad, es preciso seguir las mismas indicaciones que respecto de lo mencionado anteriormente sobre del tratamiento de datos de terceras personas.

D. En caso de niñas menores de edad donde se detecte que la persona agresora es uno de los progenitores o ambos, deben considerarse alternativas, tales como activar protocolos en coordinación con la Secretaría Nacional de Niñez, Adolescencia y Familia (SENNIAF) donde la víctima pueda ser acompañada por una persona del Departamento de Trabajo Social o Psicología. Se debe procurar que la menor se vea en la posibilidad de expresar lo que deba con plena libertad y sin temores, en este supuesto eso sería posible evitando la presencia de el o los progenitores, en tanto podrían inhibir la declaración de la víctima.

E. Es conveniente que, durante la entrevista, en la parte donde se lleva a cabo la recopilación de datos, no participe nadie más que no sea la mujer víctima de violencia y la técnica o técnico que realiza la recogida de datos. No obstante, habrá que realizar un juicio de ponderación ante la prioridad de atender otras necesidades de la persona, como puede ser apoyo de una tercera persona para facilitar una comprensión adecuada de los términos de la conversación. Por ejemplo: en los supuestos de personas con alguna discapacidad física o psíquica o en situaciones de extremo nerviosismo, ataques de pánico o ansiedad por citar posibles escenarios. En todo caso, y si se verifica la recopilación de datos en presencia de terceras personas, todo ello debe ser con la advertencia de la debida confidencialidad sobre los datos recogidos y dejando constancia en la recopilación de dicha presencia.

F. Por último, se recomienda contemplar las **excepciones que podrían autorizar el tratamiento de datos personales** previstas en el artículo 8 de la Ley No. 81 del 26 de marzo del 2019, sean los siguientes casos:

1. Datos que provengan o que se recolecten de fuentes de dominio público o accesible en medios públicos.

2. Los que se recolecten dentro del ejercicio de las funciones propias de la Administración Pública en el ámbito de sus competencias.

3. Los de carácter económico, financiero, bancario o comercial que cuenten con el consentimiento previo.

4. 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.

5. Los que son necesarios dentro de una relación comercial establecida, ya sea para la atención directa, comercialización o venta de bienes o servicios pactados.

6. 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.

7. Los casos de urgencia médica o sanitaria.

8. El tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

9. 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.

1.3. UTILIZACIÓN DE RECURSOS TECNOLÓGICOS: GRABACIÓN DE AUDIO O VIDEO

A. La grabación debe realizarse con las condiciones adecuadas de seguridad y confidencialidad. Antes de proceder a grabar, se recomienda constituir una base de datos de imágenes y/o audio proveniente de las entrevistas, y declararla dentro de las actividades de tratamiento de la institución.

B. Antes de iniciar la grabación, la mujer víctima de violencia debe ser notificada de ello, por lo que se le indicará qué se va a grabar, las personas que van a tener acceso a las grabaciones, qué finalidad tiene la grabación, cuándo se va a eliminar y si se ha constituido una base de datos para dichas imágenes o se van a guardar dentro de la base de datos relacionada con mujeres víctimas de violencia. Una vez informada, habría que recoger su consentimiento para dicha grabación.

C. Se debe mantener en relación con las grabaciones las mismas medidas de seguridad y previsión de confidencialidad que para el resto de los datos de mujeres víctimas de violencia de acuerdo con lo estipulado en la Ley No. 81 del 26 de marzo de 2019, sobre protección de datos personales.

D. Las grabaciones deben ser custodiadas cuidadosamente y la posibilidad de transferir dichos archivos o utilizarles al margen de la finalidad principal, ha de ser muy restrictiva. Es decir, cualquier posible cambio en la finalidad para la cual se recabaron los datos, deberá encontrar fundamento en una ley, de lo contrario y como parte de las garantías a favor de la víctima dispuestas en el artículo 11 de la Ley No. 81 del 26 de marzo del 2019, será indispensable que se le informe adecuadamente de esta nueva finalidad y que se le solicite su autorización. Por ejemplo: no será posible recoger datos biométricos, si la finalidad es atender su caso de violencia.

1.4. ¿QUÉ DATOS SE LE PUEDEN SOLICITAR A UNA MUJER VÍCTIMA DE VIOLENCIA?

Los datos personales que se recojan deben ser únicamente los que requiera la institución para la actuación asistencial que necesite la persona. De modo que habrá que recolectar la cantidad de datos personales que sea necesaria, proporcional y pertinente para llevar a cabo la atención que requiera la mujer.

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 estrictamente sean necesarios para ayudar a resolver la necesidad concreta.

Esta actuación, que constituye una atención correcta hacia las mujeres que enfrentan violencia, es asimismo un requisito legal en materia de protección de datos personales, debiendo limitarse la recopilación y el almacenamiento de datos a aquellos que sean proporcionados, no excesivos, adecuados y pertinentes.

2. TRATAMIENTO DE DATOS PERSONALES

2.1. ¿QUIÉN DENTRO DE LA INSTITUCIÓN TIENE ACCESO A LOS DATOS PERSONALES DE LAS MUJERES DENUNCIANTES?

Como principio esencial en el tratamiento, los datos personales deben ser accesibles sólo a aquellas personas que deben conocerlos por razón de su **rol/ participación en el proceso de atención** y esto debe estar claramente dispuesto en el manual de puestos y en los protocolos internos de la institución.

Respecto si estos datos se pueden poner en conocimiento de otras personas integrantes de la organización, se deben evaluar las siguientes posibilidades:

1. Se debe revisar si existe una **habilitación legal** para transferir los datos sin

consentimiento de acuerdo a lo dispuesto en el artículo 8 de la Ley No 81 del 26 de marzo del 2019 de protección de datos personales (ver anexo).

---

2 En caso de no existir la habilitación expresa anteriormente señalada, se debe **revisar si dentro del ordenamiento jurídico existe alguna otra norma especial de rango legal** que permita el tratamiento y posibilite dicha cesión, de ser así, será posible proceder a legalidad.

---

3 En caso de no existir habilitación legal o norma especial, se utilizará la cláusula del **consentimiento informado** para llevar a cabo la transferencia, teniendo en cuenta que dicha previsión de cesión debe ser **expresa, específica y clara.**

2.2. ¿QUÉ USOS SE LE PUEDEN DAR A ESOS DATOS PERSONALES?

Como regla general el tratamiento de los datos se va a regir por los principios de calidad/finalidad, es decir, los datos personales deben tratarse y tenerse sólo al alcance de aquellas personas que necesariamente deben conocerlos por razón de su rol y participación en el proceso de atención a la mujer víctima de violencia.

En ningún caso, salvo supuestos de excepción previstos en el artículo 8 de la Ley número 81 del 26 de marzo, sobre Protección de Datos Personales, se podrán destinar los datos a otras finalidades diferentes para las cuales se recogieron.

Esto tiene una explicación muy clara, y guarda relación con los requisitos de información y de consentimiento arriba indicados, ya que no se puede consentir lo que no se conoce. Si hemos informado a una mujer víctima de violencia de que recogemos sus datos con una finalidad de ofrecer determinado apoyo económico, por ejemplo, a la hora en que llega la persona trabajadora social, ésta no podrá utilizar los datos más que para esta finalidad. En resumen y consonancia con el artículo 11 de la citada ley, para que otras finalidades sean posibles y válidas, se requerirá del consentimiento de la víctima.

2.3. ¿ES POSIBLE CEDER DATOS DE UNA MUJER VÍCTIMA DE VIOLENCIA A OTRAS ENTIDADES?

Tras un análisis de las distintas posibilidades que existen en el panorama asistencial del Comité Nacional contra la Violencia en la Mujer (CONVIMU), sean: seguridad y protección, atención en salud, apoyo psicosocial, servicios jurídicos, ayuda económicos y asistencia material básica, entre otros, se determina lo siguiente:

La publicidad de ayudas o subsidios dirigidas exclusivamente a mujeres víctimas de violencia debe, en principio, ser restringida en cuanto a los datos que se facilitan a las personas interesadas y dirigida exclusivamente a las propias personas que participan en el proceso de otorgamiento de subvenciones. Si, **por ejemplo:** se remiten correos electrónicos, es una buena práctica colocar en "correo oculto (CO)" a las personas destinatarias, de manera que no se haga publica la información de las mismas, esto evitará futuros riesgos.

Este tipo de cesiones o transferencias, deben contar con alguna base de legitimación de acuerdo al artículo 8 de la Ley 81 del 26 de marzo del 2019 (ver anexo 1) o estar previstas en una norma especial de rango legal o, de lo contrario, deben realizarse con el consentimiento previo y explícito de la mujer víctima de violencia, que debe conocer qué cesiones concretas se van a realizar. Además, hay que tener claro que un protocolo firmado por varias instituciones no es suficiente amparo jurídico, por cuanto no es una norma de rango legal. Por ello, es preciso recabar el consentimiento de la mujer para dichas cesiones dado el especial rigor y sensibilidad de este ámbito.

En resumen, ante peticiones de datos personales de otras instituciones, participen o no en el protocolo de atención, la respuesta debe ser primero, **evaluar si se cuenta con alguna base de legitimación** de acuerdo al artículo 8 de la Ley 81 del 26 de marzo del 2019 o bien, **analizar si hay norma especial de rango legal habilitante** que permita expresamente la cesión y segundo, si no lo hubiera, analizar si se cuenta con el consentimiento de la mujer víctima de violencia o recabarlo expresamente. Si no se da alguno de estos parámetros, la cesión no deberá producirse.

Durante el tratamiento de los datos personales la única persona que sí va a poder acceder a sus datos personales, conocer cuáles datos tiene en su poder la administración, rectificar dichos datos personales si son incorrectos, oponerse a su tratamiento, solicitar su cancelación o derecho a la portabilidad, será la propia mujer en el ejercicio de sus derechos ARCO (derechos de acceso, rectificación, cancelación, oposición y portabilidad).

3. MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

3.1. MEDIDAS Y PROTOCOLOS DE SEGURIDAD DE LA INFORMACIÓN

Existen medidas de seguridad físicas y técnicas que afectan a los sistemas de tratamiento de la información. Por lo que acá es conveniente adoptar un enfoque global de la seguridad, que permita un cumplimiento íntegro de la ley, así como un tratamiento correcto de los datos de las mujeres víctimas de violencia.

Las medidas de seguridad de la información aplicables en procesos de violencia contra la mujer serán las siguientes:

A Protocolos actualizados

La primera y más importante, es contar con un documento interno de seguridad en el que definan los roles, funciones y deberes del personal, así como las implicaciones en caso de que el personal pudiera incurrir en incumplimiento. Los apartados mínimos que debe incluir el documento de seguridad son los siguientes:

- Ámbito de aplicación: especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares de seguridad.
- Funciones y obligaciones del personal.
- Estructura y descripción de las bases de datos y sistemas de información.
- Procedimiento de notificación, gestión y respuesta ante vulneraciones.
- Procedimiento para contar con copias de respaldo y recuperación de datos.
- Medidas adoptadas en el transporte, destrucción y/o reutilización de soportes y documentos.

B Capacitación constante

Una vez que contemos con el documento de seguridad, es preciso que la organización lo conozca, para ello, la capacitación continua del personal es fundamental. Para lo cual se debe incluir en los programas institucionales de capacitación, un cronograma de capacitación y actualización anual en materia de protección de datos y seguridad de la información.

C Inventarios

Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles para el personal autorizado para ello en el documento de seguridad. La salida de dichos soportes y documentos, fuera de las instituciones deberá ser autorizada por el o la responsable de la base de datos.

D Identificación y autenticación

Será necesario contar con parámetros de identificación (actuación que permite al sistema reconocer a la persona usuaria) y de autenticación (verificación que realiza el sistema sobre esta identificación, constituyendo el primer paso para garantizar el acceso únicamente de personas autorizadas).

El medio habitual de autenticación en los procesos informáticos es la utilización de contraseñas, que deben asignarse, distribuirse y almacenarse de forma que se garantice su confidencialidad e integridad, con prohibición de divulgarse entre las personas trabajadoras. Además, dichas contraseñas deben modificarse periódicamente y almacenarse de forma ininteligible.

E Copias de respaldo

Deberán establecerse procedimientos de actuación para la realización, como mínimo mensual, de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

F Accesos

De cada intento de acceso deberá guardarse información, como mínimo, la identificación de la persona usuaria, la fecha y hora en que se realizó, la base de datos accedidos, el tipo de acceso y si este ha sido autorizado o denegado.

Además de estas cuestiones, y en relación a los ficheros no automatizados, es decir, aquellas bases de datos que se tratan en papel, es importante indicar que los armarios, archivadores u otros elementos en los que se almacenen deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea necesario el acceso a los documentos. Asimismo, se deben adoptar, en el caso de tratamiento de datos en papel, medidas de control del acceso de terceras personas medidas de restricción de la realización de copias, así como control de las medidas relativas al traslado físico de la documentación.

G Vulneraciones a la seguridad

En relación a posibles vulneraciones a la seguridad de los datos personales, los responsables del tratamiento de los datos deberán cumplir con los protocolos de notificación y documentación establecidos en los artículos 37 y 38 del Decreto Ejecutivo No. 285 del 28 de mayo del 2021. **(Se adjunta a esta guía como anexo).**

3.2. MEDIDAS Y PROTOCOLOS DE SEGURIDAD DE LA INFORMACIÓN

¿CUÁNTO TIEMPO SE DEBEN CONSERVAR LOS DATOS PERSONALES?

La respuesta viene dada por la aplicación del principio de finalidad, y, por lo tanto, los datos personales de la mujer víctima de violencia podrán mantenerse en poder de la institución que los recogió siempre y cuando se mantenga la finalidad para la que se recogieron. La determinación del tiempo de atención que requiere una mujer en estas circunstancias debe ser objeto de valoración interna del organismo, y finalizado este período se procederá la eliminación de los datos. No obstante, si hay una disposición de rango legal que obligue al mantenimiento de la información con carácter indefinido, los datos personales que allí consten deberán guardarse de tal forma.

Si bien la determinación del tiempo de atención en cada caso se trata de una valoración interna, bajo ningún supuesto se trata de una decisión discrecional, ya que esa determinación debe fundamentarse en el marco jurídico del organismo, establecido en función de los valores archivísticos del documento donde constan los datos personales.

En el ámbito de los procesos legales será necesario también revisar los plazos de prescripción para exigir responsabilidades legales, en este caso, por parte de la víctima al responsable, justamente con el objetivo de garantizar que la víctima pueda ejercer sus derechos, si considera que el responsable actúo indebidamente respecto de sus datos, y que el responsable pueda defenderse ante quejas o reclamos que reciba a futuro.

Para lograr una actualización permanente de los datos personales en poder de las organizaciones, es aconsejable que éstas adopten un protocolo de revisión de estos datos, por ejemplo, mediante la puesta en contacto con la mujer víctima de violencia periódicamente para evaluar su situación y si continúa requiriendo alguna atención del servicio. Estos procesos de actualización de datos pueden consistir en buscar contacto de forma periódica con la mujer (semestral o anual) que permita confirmar su situación y su condición. En esa puesta en contacto, sería conveniente que la mujer fuera informada de la posibilidad de proceder a la cancelación de sus datos personales.

4. EJERCICIO DE LOS DERECHOS ARCO

4.1. ¿QUÉ DEBEMOS HACER PARA GARANTIZAR EL EJERCICIO DE LOS DERECHOS ARCO?

Para el ejercicio de un derecho ARCO (derechos de acceso, rectificación, cancelación, oposición y portabilidad) por parte de una mujer a la que hemos atendido, el organismo o servicio administrativo debe contar con un protocolo de actuación que establezca todos los pasos a seguir desde la recogida de la solicitud a 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 organismo o a qué 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, sin perjuicio de que pueda designar a una persona representante.

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 para resolver el derecho de acceso y no mayor de 5 días a partir de la fecha de presentación para los derechos de rectificación, cancelación y oposición) 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.

4.2. ¿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.

4.3 ¿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 Decreto Ejecutivo No. 285 del 28 de mayo del 2021, Reglamento a la Ley de Protección de Datos, 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 artículo 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 cuales 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.

9

Los datos de contacto del oficial de datos personales.

Cuando los 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.

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, Qué permite relacionar los datos entre sí, así Cómo 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.

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 especifico, 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, qué la identifica o las hace identificables.

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

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

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 efectué 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, asi 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.

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

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.

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 trasferencia.

Violación de la seguridad de los datos personales. Toda infracción a la seguridad que ocasioné la destrucción, perdida 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.

BIBLIOGRAFÍA

Organización de Estados Americanos. (1994). Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer "Convención de Belém do Pará". **https://bit.ly/3auZvsh**

Organización de Estados Americanos. (2020). Mecanismo de Seguimiento. Convención Belém do Pará. **https://bit.ly/3FzeOyM**

Organización de las Naciones Unidas [ONU]. (1979). Convención sobre la eliminación de todas las formas de discriminación contra la mujer. **https://bit.ly/3oJUgxv**

Organización de las Naciones Unidas [ONU]. (1999). Protocolo Facultativo de la Convención sobre la eliminación de todas las formas de discriminación contra la mujer. **https://bit.ly/3oLOYBo**

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

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 N.° 82 del 24 de octubre del 2013 Que adopta medidas de prevención contra la violencia en las mujeres y reforma el Código Penal para tipificar el femicidio y sancionar los hechos de violencia contra la mujer: **https://vlex.com.pa/vid/ley-n-82-24-864656264**

Ley No. 81 de 26 de marzo de 2019, sobre Protección de Datos Personales del 26 de marzo de 2019 **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/**

Programa de Naciones Unidas para el Desarrollo [PNUD]. (2018). Abordaje de la Violencia Basada en Género en Poblaciones Claves. **https://bit.ly/2YDnx29**

Organización Panamericana de la Salud. (2013). Comprender y abordar la violencia contra las mujeres: **https://apps.who.int/iris/bitstream/handle/10665/98821/WHO_RHR_12.37_spa.pdf?sequence=1&isAllowed=y**

Protocolo Nacional de Atención Integral a las Mujeres Víctimas de Violencia en las relaciones de pareja Panamá. (2016) Programa EUROsocial Programa para la Cohesión Social. Documento de Política No 37 Área: Justicia. **http://sia.eurosocial-ii.eu/files/docs/1460024082-DP_37_completo_fin.pdf**

Defensoría del Pueblo de la República de Panamá. (s.f). Observatorio Panameño contra la Violencia de Género. **https://bit.ly/2YH4m7E**

ANEXOS

1. BASES DE LEGITIMACIÓN QUE PERMITEN EL TRATAMIENTO DE DATOS PERSONALES.

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:

1. Datos que provengan o que se recolecten de fuentes de dominio público o accesible en medios públicos.
2. Los que se recolecten dentro del ejercicio de las funciones propias de la Administración Pública en el ámbito de sus competencias.
3. Los de carácter económico, financiero, bancario o comercial que cuenten con el consentimiento previo.
4. 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.
5. Los que son necesarios dentro de una relación comercial establecida, ya sea para la atención directa, comercialización o venta de bienes o servicios pactados.
6. 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.
7. Los casos de urgencia médica o sanitaria.
8. El tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

9 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, perdida, alteración, destrucción, acceso y en general, cualquier uso ilícito o no autorizado de los datos personales, aún 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 se seguridad tenga lugar en redes públicas de comunicación, se atenderá también con la seguridad pública y la defensa nacional.

REPÚBLICA DE PANAMÁ

GOBIERNO NACIONAL

AUTORIDAD NACIONAL
DE TRANSPARENCIA Y
ACCESO A LA INFORMACIÓN

www.antai.gob.pa