Política de Protección de Datos Personales

Best Doctors S.A. Empresa de Medicina Prepagada

Ecuador

Mayo 2023

Best Doctors®

BEST DOCTORS S.A. EMPRESA DE MEDICINA PREPAGADA

INDICE

I. Principios Generales de Protección de Datos Personales

Los principios generales de protección de datos personales están contemplados en el Artículo 10 de la Ley *Orgánica de Protección de Datos Personales* del Ecuador (en lo sucesivo LOPDP) y constituyen el marco de referencia de esta política.

Dicho marco de referencia permite a *Best Doctors S.A. Empresa de Medicina Prepagada* (en adelante "PPGA") tener claridad respecto al manejo adecuado de los datos personales de sus clientes, en cumplimiento de la normativa.

La presente política deberá ser observada por todos los empleados, funcionarios y ejecutivos de PPGA y hecha del conocimiento de los proveedores y terceros con los que la compañía tenga alguna relación laboral o comercial, a fin de que conozcan su alcance y cumplan con sus provisiones, en apego a la regulación aplicable en el Ecuador.

Principios

Juridicidad: Los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidos en la Constitución del Ecuador, en los instrumentos internacionales, en la LOPDP, su Reglamento y en la demás normativa y jurisprudencia aplicable.

Lealtad: El tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar clara la manera en la que se están recogiendo, utilizando, consultando o tratando sus datos personales, entre otras maneras haciendo de su conocimiento el Aviso de Privacidad de la compañía. En ningún caso los datos personales podrán ser tratados a través de medios o para fines, ilícitos o desleales.

Transparencia: El tratamiento de datos personales deberá ser transparente, por lo que toda información o comunicación relativa a su tratamiento deberá ser fácilmente accesible y entendible y deberá utilizar un lenguaje sencillo y claro.

Las relaciones derivadas del tratamiento de datos personales deben ser transparentes y deberán estar alineadas con las disposiciones de la LOPDP, su reglamento y demás normativa relacionada con la materia.

Finalidad. Las finalidades del tratamiento deberán ser explicitas, legítimas y comunicadas al titular. Ello deberá hacerse explícito mediante el Aviso de Privacidad de la compañía. No podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habilitan un nuevo tratamiento, conforme los supuestos de tratamiento legítimo señalados en la LOPDP.

Al respecto, habrá de considerarse el contexto en el que se colectaron, la información facilitada al titular en ese proceso y, en particular, las expectativas razonables del titular basadas en su relación con PPGA en cuanto a su uso posterior, la naturaleza de los datos, las consecuencias del tratamiento ulterior para el titular de los datos, y la existencia de garantías adecuadas, tanto en el tratamiento inicial, como en el tratamiento ulterior previsto.

Pertinencia y minimización de datos personales. Los datos personales que se recojan y traten deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento.

Proporcionalidad del tratamiento. El tratamiento de los datos debe ser adecuado, necesario, relevante y no excesivo con respecto a las finalidades para las cuales fueron recogidos, o bien a la naturaleza especial de los datos.

Confidencialidad. El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y privacidad y no deben tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales señaladas en la LOPDP.

Para tal efecto PPGA, en tanto responsable del tratamiento de datos personales de sus afiliados, deberá contar con las medidas técnicas y organizativas necesarias para cumplir con este principio.

Calidad y exactitud. Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros y, de ser el caso, debidamente actualizados, de tal forma que no se altere su veracidad.

La compañía debe adoptar todas las medidas razonables necesarias para que se supriman o rectifiquen -sin dilación- los datos personales que sean inexactos respecto a los fines para los que fueron se tratan.

En el caso del tratamiento de datos personales por parte de un Encargado (proveedor médico u otro tercero), PPGA deberá verificar que cuente con los controles adecuados para ello y conozca la presente política.

Siempre que PPGA haya adoptado medidas razonables para suprimir o rectificar, sin dilación los datos personales, no le será imputable la inexactitud de los mismos, siempre y cuando:

a. Hubiesen sido obtenidos por PPGA directamente del titular.

b. Hubiesen sido obtenidos por un intermediario o tercero, y ello se haga explícito en el Aviso de Privacidad entregado a los afiliados

c. Fuesen obtenidos de un registro público por parte de PPGA, en su calidad de responsable.

Conservación. Los datos personales deberán ser conservados solo durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento.

Para garantizar que los datos personales no se conserven más tiempo del necesario, PPGA, en tanto responsable del tratamiento, deberá establecer plazos para su supresión o revisión periódica.

La **conservación ampliada** de tratamiento de datos personales únicamente se realizará con fines de archivo por interés público, fines de investigación científica, histórica o estadística, siempre y cuando se establezcan las garantías de seguridad y protección de datos personales, para salvaguardar los derechos previstos en la LOPDP.

Seguridad de datos personales. PPGA, en tanto Responsable del tratamiento de los datos personales, así como los Encargados del tratamiento --por encargo de PPGA--, deberán implementar las medidas de seguridad necesarias en materia organizativa, técnica y de otra índole para proteger los datos personales frente a cualquier riesgo o vulnerabilidad, atendiendo a la naturaleza de los datos personales, al ámbito y al contexto.

Para ello, PPGA deberá firmar documentos con sus proveedores en los que establezca los controles mínimos con los que deben contar para tratar los datos de los afiliados de PPGA.

Responsabilidad proactiva y demostrada. PPGA deberá acreditar a la Autoridad de Protección de Datos Personales del Ecuador haber implementado los mecanismos necesarios para proteger los datos conforme a los principios, derechos y obligaciones establecidos en la LOPDP.

Para ello deberá valerse de estándares, mejores prácticas, esquemas de auto y co-regulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo adecuado para cumplir con los principios y las provisiones aplicables, según la naturaleza del dato y/o riesgo del tratamiento.

PPGA está obligada a rendir cuentas sobre dichas medidas al titular de los datos y a la Autoridad de Protección de Datos Personales del Ecuador.

Asimismo, informar a dicha autoridad sobre el nombramiento del Delegado de Protección de Datos, así como sobre cualquier situación que ponga en riesgo la seguridad y privacidad de los datos personales custodiados.

PPGA deberá evaluar y revisar --de forma continua-- los mecanismos que adopte para cumplir con el principio de responsabilidad proactiva y demostrada.

II. Generalidades

Conforme a la LOPDP, PPGA es responsable de proteger y limitar el uso de los datos personales que recabe de sus clientes solo para los fines para los que fueron recolectados.

Asimismo, deberá ser administradora de confianza de la data que le entreguen las personas con las que establezca o tenga una relación comercial, laboral o de negocio (afiliados, empleados, agentes, proveedores médicos y terceros).

La presente política se basa en los principios, derechos y obligaciones consignados en la LOPDP, conforme a los cuales PPGA debe tratar los datos personales.

A. ¿Qué es la información personal?

La información personal está constituida por datos que se conservan en formato electrónico o soporte físico y sirven para identificar a una persona, directa o indirectamente.

La LOPDP define los datos personales como aquellos que identifican o hacen identificable a una persona natural, directa o indirectamente, y pueden ser de las siguientes categorías:

- **Biométricos:** son datos personales únicos, relativos a las características físicas o fisiológicas de una persona natural, los cuales permiten la identificación única de dicha persona, incluyendo imágenes faciales o datos dactiloscópicos.
- **Genéticos:** Datos personales únicos relacionados con características genéticas heredadas o adquiridas de una persona natural, los cuales proporcionan información única sobre la fisiología o salud de un individuo.
- **Crediticios:** Datos que integran el comportamiento económico de las personas naturales y permiten analizar su capacidad financiera; informar sobre su solvencia patrimonial o crediticia --incluyendo el cumplimiento de obligaciones comerciales o crediticias-- y su capacidad de pago.
- **De Salud:** datos relacionados con la salud física o mental de una persona, incluidos los recabados para la prestación de servicios de atención médica.
- **Datos sensibles:** son aquellos relacionados con la etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, y aquellos de las personas apátridas y refugiadas, cuyo tratamiento indebido puede dar origen a discriminación o atentar contra los derechos y libertades fundamentales de sus titulares.

Categorías especiales de datos personales

Se considerarán categorías especiales de datos personales las siguientes:

a. Datos sensibles;

b. Datos de niñas, niños y adolescentes;

c. Datos de salud y

d. Datos de personas con discapacidad

Dichos datos deben ser manejados por los empleados de PPGA de manera confidencial y conforme a lo establecido en la presente política.

Para los fines de esta política se utilizará el término “datos personales” para referirse a la información personal de los clientes potenciales, afiliados, empleados, contratistas, solicitantes de empleo, empleados, socios comerciales y terceros.

B. Objetivo General de la política de protección de datos personales

El objetivo de la presente política es dar a conocer a los empleados, funcionarios, directores; al Delegado de Protección de Datos Personales (DPO), a los proveedores y terceros involucrados en el tratamiento de datos personales, el alcance, objetivos, lineamientos y procedimientos establecidos por PPGA para cumplir con la LOPDP y demás regulación en la materia.

C. Objetivos específicos de la política

Dar cumplimiento a lo dispuesto en la LOPDP, su reglamento y demás normativa aplicable. Para ello PPGA deberá cumplir con lo siguiente:

- Informar y capacitar a la fuerza de trabajo sobre la LOPDP y las consecuentes obligaciones de PPGA.
- Dar a conocer a la fuerza de trabajo los principios generales de la protección de datos personales,
- Establecer procedimientos, mecanismos y controles que permitan tratar de manera segura los datos personales recolectados y entregados a terceros.

D. Ley Aplicable

La LOPDP deberá ser observada por PPGA, con base en los lineamientos contenidos en la presente política, siempre que tenga lugar lo siguiente:

1. Tratamiento de datos personales en el territorio de Ecuador,
2. Tratamiento de datos por el Responsable o el Encargado domiciliados en Ecuador,
3. Tratamiento de datos de titulares que residen en el Ecuador, por parte de un Encargado no establecido en el Ecuador (BDIS)
4. Cuando al Responsable o Encargado del tratamiento --no estando domiciliados en el Ecuador--- le resulte aplicable la legislación, en virtud de un contrato o de las regulaciones vigentes del Derecho Internacional Público.

PPGA deberá incorporar medidas técnicas, de seguridad, físicas, tecnológicas y organizativas apropiadas para proteger la confidencialidad, integridad y disponibilidad de los datos personales, así como su divulgación, acceso, alteración, procesamiento, transferencia o destrucción no autorizada.

Asimismo, deberá garantizar el ejercicio de los derechos de los titulares de los datos, incluyendo el de **(i) información, (ii) acceso, (iii) rectificación y actualización, (iv) eliminación, (v) oposición, (vi) portabilidad, (vii) suspensión del tratamiento, (viii) y no ser objeto de una decisión basada** única o parcialmente en **valoraciones automatizadas**.

PPGA podrá anonimizar los datos personales bajo su resguardo, en cuyo caso no le serán aplicables las disposiciones de la LOPDP. Sin embargo, en cuanto los datos dejen de estar disociados (anonimizados), PPGA deberá observar la regulación, incluyéndo el tratamiento sobre una base de licitud.

E. Alcance de la política

La presente política es de cumplimiento obligatorio para todas las áreas, empleados, funcionarios, directivos, proveedores u otros terceros involucrados en el tratamiento de datos personales, por encargo de PPGA, y que por ese motivo sean considerados como Encargados del Tratamiento.

El incumplimiento de esta política puede tener como consecuencia el deterioro de la confianza de los afiliados, el daño reputacional a la compañía, o sanciones administrativas o penales. Por ello, los empleados, directivos y terceros con los que PPGA tenga una relación contractual podrían enfrentar consecuencias que van desde las acciones disciplinarias, la recisión del contrato hasta las demandas judiciales.

III. Roles y Responsabilidades

LOPDP contempla tres figuras con roles claves para el cumplimiento de sus disposiciones, las cuales deberán ser observadas por PPGA:

- El Delegado de Protección de Datos Personales
- El Responsable del Tratamiento de Datos Personales, y
- El Encargado del Tratamiento de Datos Personales.

A. El Delegado de protección de datos personales (DPO)

Es la persona natural encargada de informar al Responsable del tratamiento de los datos personales sobre sus obligaciones en materia de protección de datos, así como de supervisar el cumplimiento de la normativa y cooperar con la Autoridad de Protección de Datos Personales del Ecuador, sirviendo como punto de contacto entre ésta y la entidad responsable del tratamiento de los datos (PPGA).

PPGA deberá nombrar a un Delegado de Protección de Datos Personales que conozca de la materia y esté familiarizado con las actividades de la compañía, a fin de que ejercer las funciones señaladas por la normativa.

A1. Obligaciones del Delgado de protección de datos personales

El Director Ejecutivo de PPGA, con asesoría interna y externa especializada, deberá nombrar a un DPO y verificar que cumpla con las obligaciones consignadas en la LOPDP, incluyendo:

1. Asesorar al personal de PPGA involucrado en el tratamiento de datos personales sobre el alcance y las provisiones de la presente política, así como respecto a las disposiciones contenidas en la LOPDP, su reglamento y otras disposiciones aplicables.

2. Supervisar el cumplimiento de las disposiciones referidas, así como las que emita la Autoridad de Protección de Datos Personales del Ecuador;

3. Asesorar en el análisis de riesgo, evaluación de impacto y medidas de seguridad aplicadas por PPGA y supervisar su aplicación;

4. Cooperar con la Autoridad de Protección de Datos Personales y actuar como punto de contacto con dicha entidad respecto al tratamiento de datos personales por parte de PPGA y sus encargados de tratamiento;

5. Acreditar ante la autoridad haber implementado mecanismos para la protección de datos personales, con base en las mejores prácticas, incluyendo esquemas de auto-regulación y co-regulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo adecuado para el dato y el riesgo del tratamiento.

6. Rendir cuentas al titular de los datos personales y al a Autoridad de Protección de Datos Personales cuando sea necesario.

7. Supervisar que PPGA cuente con plazos para la supresión de los datos personales con miras a no conservarlos más allá del tiempo necesario para cumplir con el fin para el que fueron recabados.

8. Evaluar los mecanismos que haya adoptado PPGA para cumplir con el manejo adecuado y protección de los datos personales bajo su custodia.

9. Establecer mecanismos para que en un plazo no mayor a 15 días el titular de los datos tenga acceso a sus datos, sin necesidad de justificación.

10. Garantizar que sea atendido el derecho del titular de los datos a suprimirlos cuando el tratamiento no cumpla con los principios establecidos en la LOPDP; cuando no sea necesario para el cumplimiento de la finalidad para la cual fue otorgado el consentimiento; cuando hayan cumplido su finalidad; cuando haya vencido el plazo de conservación establecido por la compañía; cuando afecte derechos o libertades fundamentales; cuando el titular revoque el consentimiento o señale no haberlo otorgado para uno o varios fines específicos; o bien cuando exista una obligación legal.

11. Implementar métodos para eliminar, hacer ilegible o volver irreconocibles de forma definitiva y segura los datos personales. El DPO deberá velar que PPGA cumpla con esta obligación en el plazo no mayor a 15 días tras recibir la solicitud.

12. Facilitar el derecho de portabilidad del titular de los datos, otorgándolos en formato compatible, actualizado, estructurado e inter-operable y de lectura mecánica, preservando sus características o transmitirlos a otros responsables.

13. Negar la rectificación, actualización, eliminación, oposición, anulación o portabilidad de los datos solo en los siguientes casos:

    a. Cuando el solicitante no sea el titular de los datos personales, o su representante legal no se encuentre debidamente acreditado.

    b. Cuando los datos sean necesarios para el cumplimiento de una obligación legal o contractual, o una orden judicial, resolución o mandato motivado por autoridad pública competente;

    c. Cuando los datos sean necesarios para la formulación, ejercicio o defensa de reclamos o recursos;

    d. Cuando se pueda causar perjuicios o afectar intereses legítimos de terceros, y ello sea acreditado por el responsable de la base de datos (PPGA) al momento de dar respuesta al titular respecto a su solicitud de ejercicio de dicho derecho;

    e. Cuando puedan ser obstaculizadas actuaciones judiciales o administrativas en curso;

    f. Cuando los datos sean necesarios para ejercer el derecho a la libertad de expresión y opinión;

    g. Cuando los datos sean necesarios para proteger el interés vital del interesado o de otra persona natural;

    h. En los casos en los que medie el interés público, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta Ley y a los criterios de legalidad, proporcionalidad y necesidad;

    i. En el tratamiento de datos personales que sean necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística.

14. Suspender el tratamiento de los datos personales en los siguientes casos:

    a. Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de los mismos;

    b. Cuando el tratamiento sea ilícito y el interesado se oponga a su supresión y solicite la limitación de su uso;

    c. Cuando el responsable (PPGA) ya no necesite los datos personales para los fines para los que fueron colectados, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; y,

    d. Cuando el titular así lo solicite, si impugna la exactitud de los datos y mientras se verifican (deberá colocarse en la base de datos haciendo constar que la información ha sido impugnada). Asimismo, cuando PPGA ya no necesite los datos personales para los fines para los que fueron recabados.

15. Otorgar acceso, rectificación, actualización o eliminación de los datos de una persona fallecida, a petición del titular de los derechos sucesorios, siempre que el titular de los datos no haya indicado en vida otro uso o destino para sus datos. En caso de fallecimiento de niñas, niños, adolescentes o personas que la ley reconozca como incapaces, las facultades de acceso, rectificación, actualización o eliminación podrán ser ejercidas solo por quien hubiese sido su último representante legal.

16. Implementar un proceso de verificación, evaluación y valoración de la eficiencia, eficacia y efectividad de las medidas técnicas y organizativas implementadas por PPGA, con objeto de garantizar y mejorar la seguridad del tratamiento de los datos personales.

17. Evidenciar que las medidas implementadas por PPGA mitiguen de forma adecuada los riesgos utilizando, entre otras:

    a. La anonimización, seudonomización o cifrado de los datos personales;

    b. Mecanismos para mantener la confidencialidad, integridad y disponibilidad de los sistemas de tratamiento de los datos para tener acceso a ellos de forma rápida en caso de incidentes,

18. Notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y a la ARCOTEL tan pronto como sea posible y a más tardar 4 días después de que se haya tenido constancia de ella.

19. Notificar la vulneración de la seguridad de los datos personales al titular cuando conlleve un riesgo a sus derechos fundamentales y dentro de los 3 días contados a partir de la fecha en la que se tuvo conocimiento de ésta. No será necesario hacerlo si el responsable adoptó medidas de protección apropiadas respecto a los datos afectados; se garantice que el riesgo para los derechos fundamentales no ocurrirá; o cuando se requiera un esfuerzo desproporcionado, en cuyo caso se deberá hacer una comunicación pública a través de cualquier medio para informar de la vulneración de seguridad de los datos.

20. Verificar que se suscriban contratos de confidencialidad y manejo adecuado de datos personales con el Encargado del tratamiento (proveedores médicos y terceros) de datos personales.

21. Permitir y contribuir a la realización de auditorías e inspecciones por parte de un auditor acreditado por la Autoridad de Protección de Datos Personales.

22. Reportar y mantener actualizada la información ante la Autoridad de Protección de Datos Personales incluyendo el domicilio legal y los datos de contacto del Responsable y los Encargados del tratamiento de los datos, la finalidad de su tratamiento, naturaleza de los mismos, los medios utilizados para protegerlos, las herramientas administrativas técnicas, organizativas y jurídicas implementadas para garantizar su seguridad y su tiempo de conservación.

B. El Responsable del tratamiento de datos personales

Se refiere a la persona natural o jurídica, pública o privada, que solo o con otros decide sobre la finalidad y el tratamiento de los datos personales.

B1. Obligaciones de PPGA como Responsable del tratamiento de datos personales

1. Tratar los datos personales en estricto apego a los principios y derechos consagrados en la LOPDP, su reglamento y en las directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales;

2. Aplicar e implementar controles y herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, a fin de garantizar y demostrar que el tratamiento de los datos se ha realizado conforme a lo previsto en la LOPDP y demás normativa aplicable;

3. Implementar procesos de verificación, evaluación y valoración periódica de la eficiencia, y efectividad de las herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas;

4. Utilizar metodologías de análisis y gestión de riesgos;

5. Realizar evaluaciones de seguridad respecto al tratamiento de datos personales;

6. Implementar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas para prevenir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas;

7. Notificar a la Autoridad de Protección de Datos Personales y al titular de los datos acerca de cualquier violación a la seguridad en el tratamiento de sus datos personales,

8. Suscribir contratos de confidencialidad y manejo adecuado de los datos personales con el Encargado del tratamiento;

9. Asegurar que los encargados del tratamiento de datos personales ofrezcan mecanismos suficientes para garantizar su protección conforme a lo establecido en la LOPDP, su Reglamento, así como en las directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, y las mejores prácticas internacionales;

10. Mantener actualizado el “Registro Nacional de Protección de Datos Personales”, de conformidad a lo dispuesto en la LOPDP y su Reglamento;

11. Permitir y contribuir a la realización de auditorías o inspecciones por parte de la Autoridad de Protección de Datos Personales.

C. El Encargado del tratamiento de datos personales

Se refiere a la persona, natural o jurídica, pública o privada, que sola o conjuntamente trata o procesa datos personales a nombre del PPGA.

C1. Obligaciones del Encargado de tratamiento de datos personales.

Tendrá las mismas obligaciones que el Responsable del tratamiento en lo que le sea aplicable conforme a la LOPDP y su Reglamento.

Los proveedores de PPGA, en su calidad de encargados del tratamiento de datos personales, deberán firmar un contrato en el que se establezca de manera clara y precisa que tratarán los datos conforme a la regulación aplicable y no los utilizarán para finalidades diferentes a las señaladas en el contrato, ni los transferirán a otras personas o entidades.

Una vez cumplida la prestación contractual con PPGA, los datos personales en poder del Encargado deberán ser destruidos o devueltos a PPGA.

IV. Medidas de Seguridad

La seguridad de la información y una debida administración de riesgos en materia de protección de datos personales son componentes esenciales con los que PPGA debe contar para cumplir con la LOPDP.

Por ello, PPGA deberá implementar salvaguardas de seguridad de la información para proteger la información personal que recopile, almacene y procese frente a accesos, usos, divulgación o destrucción no autorizados, así como frente a otras amenazas de seguridad (internas como externas) a fin de evitar multas, sanciones, litigios o daños a la reputación de la compañía. ELIO

A. Seguridad de los datos personales

PPGA, en su calidad de Responsable del tratamiento de los datos personales, al igual que los encargados, deberán garantizar la seguridad de los datos tomando en cuenta sus categorías y volumen; las mejores prácticas, el contexto y los fines del tratamiento.

PPGA deberá implementar un proceso de verificación, evaluación y valoración continua de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de otra índole, implementadas para garantizar la seguridad de los datos.

PPGA y los encargados del tratamiento de datos personales deberán evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados.

B. Medidas que pueden ser implementadas para mitigar riesgos identificados:

1. Anonimización, seudonomización o cifrado de datos personales;
2. Medidas para mantener la confidencialidad, integridad y disponibilidad inmediata de los datos personales almacenados;

PPGA, en su calidad de Responsable del tratamiento de los datos y, en su oportunidad, el Encargado del tratamiento, deberán tomar las medidas necesarias, de forma permanente y continua, para evaluar, prevenir, impedir, reducir, mitigar y controlar los riesgos y amenazas a los derechos de los titulares de los datos.

C. Análisis de riesgo, amenazas y vulnerabilidades

PPGA deberá utilizar y verificar que los encargados del tratamiento (proveedores) incorporen metodologías que tomen en cuenta:

1. Las particularidades del tratamiento;
2. Las particularidades de las partes involucradas; y,
3. Las categorías y el volumen de datos personales objeto de tratamiento.

C1. Amenazas internas a la seguridad de los datos

Existen distintos tipos de amenazas internas a la seguridad de los datos personales. PPGA deberá evitar que éstos sean vulnerados de manera accidental, negligente o maliciosa por

Las **amenazas maliciosas** de carácter interno suponen la intención de hacer daño y actuar inapropiadamente.

Las **amenazas por negligencia** no suponen la intención de hacer daño, pero requieren una decisión clara para actuar, la cual plantea un riesgo.

Las **amenazas accidentales** no buscan hacer daño, ni tienen una decisión consciente de actuar de cierta manera, sino que son resultado de errores que afectan la seguridad de los datos.

PPGA deberá establecer procedimientos para capacitar a su personal para evitar este tipo de amenazas y aplicar las medidas correctivas necesarias, según sea el caso.

C2. Amenazas de Seguridad Externa

Los ataques a la seguridad de la información provienen, en su mayoría, de actores y amenazas externas que son capaces de vulnerar la red y los sistemas de protección.

Con el fin de atender las amenazas de seguridad externa PPGA deberá apegarse a la política de seguridad de la información de BDI.

PPGA deberá implementar protocolos de seguridad, en coordinación con BDI, para prevenir y minimizar las amenazas externas a la seguridad de la información y capacitar a su personal en la materia.

D. Evaluación de impacto del tratamiento de los datos personales

Las evaluaciones de impacto del tratamiento de datos personales son esenciales para prevenir riesgos y realizar ajustes a los sistemas de seguridad de la información.

El DPO de PPGA deberá coordinar la implementar de procedimientos periódicos de evaluación de impacto del tratamiento de datos personales que le permita identificar y resolver las posibles deficiencias de protección de la información, y con ello reducir el riego de costos asociados y el daño reputacional.

Asimismo, PPGA deberá realizar dicha evaluación cuando haya identificado la posibilidad de que el tratamiento de datos conlleve un alto riesgo para los derechos y libertades de su titular.

Una evaluación de impacto será obligatoria cuando tenga lugar lo siguiente:

a. Una evaluación sistemática de datos personales de forma automatizado, como puede ser la elaboración de perfiles, sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales;

b. Un Tratamiento a gran escala de las categorías especiales de datos;

c. La Observación sistemática a gran escala de una zona de acceso público.

E. Incidentes de datos personales

Ocurren cuando ha sido o se cree que pudo haber sido divulgada información personal a un tercero sin autorización.

Se trata de una posible filtración de datos causada por la pérdida, mal uso, extravío o acceso no autorizado a los datos personales.

Los incidentes de datos personales pueden contribuir a identificar fraudes, robo, pérdidas financieras u otro tipo de daños, pero afectan a la organización por la falta de confianza que generan, la afectación a los titulares de los datos, las publicaciones negativas en prensa; las multas que pueden acarrear, así como las consecuencias más graves derivadas de la pérdida masiva de datos, si no se reportan y administran de forma oportuna.

Todos los empleados de PPGA, responsables de tratar datos personales, deberán seguir procedimientos de administración de incidentes incluyendo la oportuna notificación a quien corresponda, así como el control de daños.

Los procedimientos de administración de incidentes deberán incluir lo siguiente:

1. Reporte al DPO y al área de cumplimiento de BDIS con detalles sobre el incidente;
2. Investigación del incidente;
3. Determinación de si se produjo una filtración, extracción u otra forma de pérdida de datos personales.
4. Notificación a la Autoridad de Datos Personales conforme al procedimiento establecido por el DPO.
5. Documentación del incidente incluyendo las evidencias con las que cuente.

F. Notificación a la Autoridad de Protección de Datos Personales

PPGA deberá notificar la vulneración de la seguridad de datos a la Autoridad de Protección de Datos Personales y a ARCOTEL, tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de cinco (5) días, deberá ir acompañada de indicación de los motivos de la dilación.

Por su parte, los proveedores de PPGA, encargados de tratar datos personales, deberán notificarle cualquier vulneración a la seguridad de los datos a más tardar en dos (2) días contados a partir de la fecha en que se tuvo conocimiento de la vulneración.

G. Atención a emergencias e incidentes informáticos

En caso de una emergencia o incidente informático, PPGA deberá colaborar con las autoridades competentes y con los equipos de respuesta a incidentes de seguridad y de emergencias informáticas.

Los prestadores de servicios de telecomunicaciones, de tecnologías de la información y de seguridad podrán acceder y efectuar tratamiento a los datos personales contenidos en las notificaciones de vulneración a la seguridad para detectar, analizar y proteger la información, así como para adoptar medidas de seguridad proporcionales a los riesgos identificados.

H. Notificación de vulneración de seguridad al titular

PPGA, en su carácter de responsable del tratamiento de datos personales, deberá notificar sin dilación la vulneración de seguridad de datos personales al titular cuando conlleve un riesgo a sus derechos fundamentales y libertades individuales, dentro del término de tres días contados a partir de la fecha en la que tuvo conocimiento del riesgo.

H1. Excepción a la notificación de la vulneración de seguridad

1. Cuando PPGA haya adoptado medidas de protección técnicas organizativas o de cualquier otra índole apropiadas. La excepción será calificada por la Autoridad de Protección de Datos.
2. Cuando PPGA haya tomado medidas que garanticen que el riesgo a los derechos fundamentales y libertades individuales del titular no ocurrirá. La Autoridad de Protección de Datos confirmará la procedencia de esta excepción.
3. Cuando se requiera un esfuerzo desproporcionado para hacerlo; en cuyo caso PPGA deberá realizar una comunicación pública en la que informe la vulneración de la seguridad de los datos personales bajo su custodia.

V. Medidas Organizativas de Control

A. Implementación de Políticas y Procedimientos Locales.

En suplementación a la presente política, el DPO y el área de cumplimiento de BDI podrán definir procesos, procedimientos y guías para cumplir con lo dispuesto en la LOPDP, su reglamento y disposiciones aplicables.

Todos los suplementos relacionados y que se añadan deberán ser revisados y aprobados por el delegado de protección de datos personales y el área de cumplimiento para asegurar la coherencia con esta política.

B. Obligación de reportar al Registro Nacional de protección de datos personales

PPGA en su calidad de responsable del tratamiento de datos personales deberá reportar y mantener actualizada la información ante la Autoridad de Protección de Datos Personales, sobre lo siguiente:

1. Identificación de la base de datos o del tratamiento;
2. El nombre domicilio legal y datos de contacto de PPGA en su calidad de responsable o de encargado del tratamiento de datos personales;
3. Características y finalidad del tratamiento de datos personales;
4. Naturaleza de los datos personales tratados;
5. Identificación, nombre, domicilio legal y datos de contacto de los destinatarios de los datos personales, incluyendo encargados y terceros;
6. Modo de interrelacionar la información registrada;
7. Medios utilizados para implementar los principios, derechos y obligaciones contenidas en la LOPDP y normativa especializada;
8. Requisitos y herramientas administrativas técnicas y físicas, organizativas y jurídicas implementadas para garantizar la seguridad y protección de datos personales;
9. Tiempo de conservación de los datos.

C. Obligaciones de a cada área de PPGA

- Identificar los datos personales maneja cotidianamente
- Clasificar los datos personales según lo establecido en la LOPDP
- Implementar los procesos y controles en las operaciones cotidianas de PPGA para disuadir, detectar y prevenir riesgos potenciales en materia de protección de datos personales.

D. Funciones de Supervisión – Cumplimiento/ Auditoría

Los riesgos en materia de protección de datos personales también se rigen por las funciones de supervisión de PPGA, para lo cual deberá atender lo siguiente:

D1. Cumplimiento.

En coordinación con el DPO, PPGA será responsable de:

- Supervisar que la administración de controles que se implemente mitigue riesgos relacionados con la protección de datos personales en cada operación de PPGA.
- Asesorar a los departamentos de negocio y otras áreas corporativas funcionales respecto a las disposiciones legales aplicables en materia de protección de datos personales.
- Qué los empleados tengan información suficiente y conozcan la existencia de la Ley Orgánica de Protección de datos personales, su reglamento y demás disposiciones aplicables.
- Verificar que la operación tenga un programa acorde y relativo a su área relacionado con el cumplimiento de la protección de datos personales.
- En coordinación con el Delegado de Protección de Datos Personales podrá realizar evaluaciones de riesgo.
- Compartirá resultados de sus actividades a las juntas o comités correspondientes.

D2. Auditoría Interna

PPGA será responsable de validar la efectividad y fuerza de los controles implementados y proporcionar una evaluación objetiva, en conjunto con el DPO.

VI. Aviso, Consentimiento y Control

A. Aviso

PPGA deberá proporcionar aviso a sus clientes sobre la recopilación y tratamiento de datos personales a través de un Aviso de Privacidad, el cual consiste en un documento físico, electrónico generado por PPGA que se pone a disposición del titular de datos personales, previo al tratamiento de los mismos.

El Aviso debe brindar una explicación de los datos personales que se recopilan, el fin del tratamiento, las razones y la manera en la que se utilizarán, protegerán y con quién podrán compartirse.

B. Consentimiento

Obtener consentimiento del titular de los datos personales

Con objeto de mantener la confianza de los clientes, empleados y del público en general, PPGA tiene la obligación de cuidar adecuadamente los datos personales y el ejercicio de los derechos otorgados por la LOPDP y demás regulación aplicable en la materia.

El consentimiento que PPGA debe obtener debe basarse en la manifestación de la voluntad libre, específica, informada e inequívoca del titular de los datos personales de autorizar al responsable del tratamiento a tratar los mismos.

PPGA deberá obtener el consentimiento del titular de los datos siempre que sea necesario utilizar sus datos personales, para lo cual PPGA deberá obtener dicha autorización antes de:

- Recopilar, usar o procesar información personal
- Compartir la información personal del titular con cualquier tercero
- Transferir la información personal del titular fuera del Ecuador
- Utilizar la información personal para comercializar los bienes o servicios de PPGA, ya sea directa o indirectamente
- Utilizar o colocar web cookies en la computadora u otros dispositivos electrónicos del titular de datos personales

B1. Excepciones para la transferencia o comunicación de datos personales

No será necesario contar con el consentimiento del titular para la transferencia o comunicación de datos personales, en los siguientes supuestos:

1. Cuando los datos han sido recogidos de fuentes accesibles al público;
2. Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica entre el responsable de tratamiento y el titular, cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con base de datos. En este caso la transferencia o comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique;
3. Cuando los datos personales deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la norma vigente;
4. Cuando la comunicación se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando dichos datos se encuentren debidamente disociados o a lo menos anonimizados, y,
5. Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que implique intereses vitales de su titular y este se encontrare impedido de otorgar su consentimiento.
6. Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para realizar los estudios epidemiológicos de interés público, dando cumplimiento a los estándares internacionales en la materia de derechos humanos, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad.

C. Control

Los derechos de los titulares de los datos deben ser respetados; por lo tanto es indispensable que PPGA observe las siguientes medidas de control y cumplimiento de la normativa:

Proporcionar a todo el público, titulares de datos personales el Aviso de privacidad antes o durante la recopilación de información personal y actualizar dicho aviso en caso de que el negocio modifique la manera en que utiliza, comparte o procesa la información personal.

Obtener el consentimiento por parte de los titulares personas naturales antes de procesar los datos personales y que sea consistente con cualquier aviso de privacidad previamente proporcionado.

Contar con un formato para que los titulares otorguen el consentimiento por escrito y firmado para el tratamiento de su información.

Contar con un mecanismo para revocar el consentimiento que sea sencillo y garantice celeridad, eficiencia, eficacia y gratuidad. El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación.

Dejar de procesar los datos personales de un individuo dentro del tiempo establecido por la LOPDP, su reglamento y demás disposiciones aplicables.

Proporcionar a los titulares acceso a su información personal para su revisión y actualización, para lo cual PPGA deberá contar con un procedimiento sencillo para ser contactada y recibir solicitudes de acceso, rectificación y actualización, eliminación, oposición, portabilidad.

Evitar tratar datos personales con fines distintos para los que fueron recopilados.

Contar con un procedimiento que permita la atención al titular de los datos personales cuando éste presente cualquier requerimiento, petición, queja o reclamación directamente y relacionado con el ejercicio de sus derechos.

D. Valoraciones Automatizadas

PPGA deberá considerar, en el marco de sus procedimientos operativos el derecho que tiene el titular de datos personales a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o que atenten contra sus derechos y libertades fundamentales.

No se aplicará este derecho cuando:

1. La decisión es necesaria para la celebración o ejecución de un contrato entre el titular y el PPGA o con el encargado del tratamiento de datos personales (algún proveedor médico).
2. Esté autorizada por la normativa aplicable, orden judicial, resolución o mandato motivado de autoridad técnica competente, para lo cual se deberá establecer medidas adecuadas para salvaguardar los derechos fundamentales y libertades del titular.
3. Se base en el consentimiento explícito del titular.
4. La decisión no conlleve impactos graves o riesgos verificables para el titular. No se podrá exigir la renuncia a este derecho en forma adelantada a través de contratos de adhesión masivos. A más tardar en el momento de la primera comunicación con el titular de los datos personales, para informar una decisión basada únicamente en valoraciones automatizadas, este derecho le será informado explícitamente por cualquier medio idóneo.

E. Tratamiento adecuado y legítimo de los datos personales

PPGA deberá supervisar que el tratamiento de los datos sea:

a. realizado con consentimiento del titular para una o varias finalidades específicas.
b. para el cumplimiento de obligaciones legales,
c. para el cumplimiento de una orden judicial
d. para la ejecución de medidas pre-contractuales a petición del titular
e. para el cumplimiento de obligaciones contractuales.
f. Para proteger intereses vitales del interesado o de otra persona natural, como su vida, salud o integridad.
g. Para tratamiento de datos personales que consten en bases de datos de acceso público
h. Para satisfacer un interés legítimo del responsable de tratamiento o de tercero, siempre que no prevalezca el interés o derechos fundamentales.

E1. Tratamiento de datos sensibles

PPGA podrá tratar datos sensibles únicamente cuando concurra alguna de las siguientes circunstancias:

a. El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, a través del Aviso de Privacidad.

b. El tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos de PPGA en su calidad de responsable del tratamiento de datos personales del titular en el ámbito del Derecho laboral y de la seguridad y protección social.

c. El tratamiento sea necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento.

d. El tratamiento se refiera a datos personales que el titular ha hecho manifiestamente públicos.

e. El tratamiento sea realizado por orden de autoridad judicial.

f. El tratamientosea necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.

g. Cuando el tratamiento de los datos de salud se sujete a las disposiciones contenidas en la LOPDP.

E2. Tratamiento de datos de niñas, niños y adolescentes

PPGA no podrá tratar datos sensibles o datos de niñas, niños y adolescentes a menos que se cuente con la autorización expresa del titular o de su representante legal.

Los adolescentes, en ejercicio progresivo de sus derechos, a partir de los 15 años, podrán otorgar, en calidad de titulares, su consentimiento explícito para el tratamiento de sus datos personales, siempre que se les especifique con claridad sus fines.

E3. Tratamiento de Datos Personales de Personas Fallecidas

Los titulares de derechos sucesorios de las personas fallecidas podrán dirigirse PPGA con el objeto de solicitar el acceso, rectificación y actualización o eliminación de los datos personales del titular de datos personales fallecido (causante), siempre que el titular de los datos no haya, en vida, indicado otra utilización o destino para sus datos.

Las personas o instituciones que la persona fallecida haya designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de ésta y, en su caso, su rectificación, actualización o eliminación.

En caso de fallecimiento de niñas, niños, adolescentes o personas que la ley reconozca como incapaces, las facultades de acceso, rectificación, actualización o eliminación podrán ser ejercidas por quien hubiese sido su último representante legal.

E4. Tratamiento de Datos crediticios

PPGA podrá tratar datos crediticios cuando los mismos sean obtenidos de fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor. Tales datos no deberán ser comunicados o difundidos, ni podrán tener una finalidad secundaria.

E5. Tratamiento de Datos de Salud

PPGA está sujeta al deber de confidencialidad, de tal manera que garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas organizativas apropiadas.

Casos en los que no se requiere consentimiento del titular para el tratamiento de datos de salud.

No se requerirá el consentimiento del titular para el tratamiento de datos de salud cuando ello sea necesario por razones de interés público esencial en el ámbito de la salud, el que en todo caso deberá ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.

Parámetros para el tratamiento de datos relativos a la salud

Todo tratamiento de datos relativos a la salud que realice PPGA deberá cumplir con los siguientes parámetros mínimos:

1. Los datos relativos a la salud generados en establecimientos de salud privados serán tratados cumpliendo los principios de confidencialidad y secreto profesional. El titular de la información deberá brindar su consentimiento previo salvo en los casos en que el tratamiento sea necesario para proteger intereses vitales del interesado, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; o sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria, y social, sobre la base de la legislación especializada sobre la materia o en virtud de un contrato con un profesional sanitario. En este último caso el tratamiento sólo podrá ser realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con la legislación especializada sobre la materia o con las demás normas que al respecto pueda establecer la Autoridad.
2. Los datos relativos a la salud, siempre que sea posible, deberán ser previamente anonimizados o seudonomizados, evitando la posibilidad de identificar a los titulares de los mismos.
3. El tratamiento de datos de salud anonimizados deberá ser autorizado por la Autoridad de Protección de Datos Personales, con base en un protocolo técnico que contenga los parámetros necesarios que garanticen la protección de dichos datos.

VII. Terceros. Procesamiento de datos

En muchos casos, por la naturaleza de los servicios que ofrece PPGA, se requiere la transferencia de datos personales a terceros, lo cual solo podrá hacerse cuando se requieran para el cumplimiento de fines directamente relacionados con el contrato y se cuente con el consentimiento del titular, con base en el formato de consentimiento y en el Aviso de Privacidad, que deberán entregarse a los afiliados.

El tratamiento de datos personales realizado por terceros como BDIS o proveedoresmédicos de PPGA, deberá estar regulado por un contrato en el que se establezca de manera clara y precisa que el encargado del tratamiento lo hará únicamente conforme las instrucciones del responsable (PPGA) y no los utilizará para finalidades diferentes a las señaladas en el contrato.

A. Procedimiento para cada nueva contratación o renovación de contrato con tercero

PPGA deberá realizar un análisis antes de celebrar o renovar un contrato, basado en tres pasos:

- **Primer Paso -** Realizar una evaluación preliminar de riesgo.
- **Segundo Paso -** Realizar una revisión de las medidas de seguridad con las que cuenta el tercero.
- **Tercer Paso -** Incluir en el contrato o convenio disposiciones o cláusulas relacionadas con protección de datos personales.

Primer Paso – Verificar si el tercero recopilará, accederá, compartirá, utilizará, visualizará o almacenará los datos personales que han sido entregados a PPGA.

Segundo Paso – PPGA deberá solicitar el apoyo del área técnica de TI para asegurarse que el tercero cuente con medidas de seguridad adecuadas para proteger la información, con base en un documento formulario. que se designe para tal caso, deberán tomarse las decisiones respecto a la contratación de servicios con el tercero analizado.

Tercer Paso - El área legal, en coordinación con el DPO deberá incorporar en los contratos disposiciones de protección de datos según lo requerido por la LOPDP.

VIII. Transferencia Transfronteriza de datos

PPGA deberá estar al tanto de las obligaciones que debe cumplir conforme a la LOPDP, respecto a la transferencia transfronteriza de datos personales, así como considerar si existe alguno de los mecanismos necesarios para soportar la transferencia conforme lo dispuesto en la LOPDP, su reglamento y normativa vigente

1. Que exista un acuerdo para la transferencia de datos con la parte que tendrá acceso u obtendrá la información personal
2. Notificar a la Autoridad de Protección de Datos
3. Contar con el consentimiento o notificar al titular de los datos a ser transferidos

La transferencia internacional de datos personales deberá sujetarse a lo dispuesto en la LOPDP, incluyendo:

A. La transferencia a países declarados como nivel adecuado de protección

Se podrán transferir o comunicar datos personales a países, organizaciones y personas jurídicas en general que brinden niveles adecuados de protección, y que se ajusten a la obligación de cumplimiento y garantía de estándares reconocidos internacionalmente conforme a los criterios establecidos en el Reglamento de la LOPDP. Será la Autoridad de Protección de Datos Personales quien tendrá la obligación de emitir información de consulta para tal fin.

B. Transferencia o comunicación mediante garantías adecuadas

En caso de realizar una transferencia internacional de datos a un país, organización o territorio económico internacional que no haya sido calificado por la Autoridad de Protección de Datos de tener un nivel adecuado de protección, PPGA podrá realizar la referida transferencia internacional siempre que, en su calidad de responsable, ofrezca garantías adecuadas para el titular, para lo cual se deberá observar lo siguiente:

C. Autorización para transferencia internacional

Cuando PPGA necesite realizar una transferencia internacional de datos personales requerirá la autorización de la Autoridad de Protección de Datos, para lo cual deberá garantizar documentadamente el cumplimiento de la normativa vigente sobre protección de datos personales.

La información sobre transferencias internacionales de datos personales deberá ser registradas previamente en el “Registro Nacional de Protección de Datos Personales”.

D. Casos excepcionales de transferencias o comunicaciones internacionales

Se podrá realizar transferencias o comunicaciones internacionales de datos personales, en los siguientes casos:

1. Cuando el titular haya otorgado su consentimiento explícito a la transferencia o comunicación propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias o comunicaciones internacionales, debido a la ausencia de una resolución de nivel adecuado de protección y de garantías adecuadas.
2. Cuando la transferencia internacional tenga como finalidad el cumplimiento de una obligación legal o regulatoria.
3. Cuando la transferencia internacional necesaria para la ejecución de un contrato entre el titular y el responsable del tratamiento de datos personales, o para la ejecución de medidas de carácter precontractual adoptadas a solicitud del titular.

4. Cuando la transferencia internacional de datos personales sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento.

PPGA contará con un término de diez (10) días para contestar, notificar y ejecutar lo que corresponda.

IX. Educación Digital y Capacitación

PPGA en su calidad de responsable de la protección de datos personales deberá desarrollar y brindar capacitación sobre esta política a sus empleados.

La capacitación podrá brindarse a través de cursos en línea o presenciales y como buena práctica deberá realizarse de forma anual dejando constancia de las evaluaciones aplicadas para efectos de auditoría.

Adicionalmente el DPO, en coordinación con el área de Cumplimiento y Operaciones, deberá comunicar internamente las provisiones de la LOPDP y las disposiciones de la presente política.

X. Glosario de términos y equivalencias

- **Autoridad de Protección de Datos Personales:** Autoridad pública independiente encargada de supervisar la aplicación de la LOPDP, reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales.
- **Anonimización:** La aplicación de medidas dirigidas a impedir la identificación o reidentificación de una persona natural, sin esfuerzos desproporcionados.
- **Base de datos o fichero:** Conjunto estructurado de datos cualquiera que fuera la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica.
- **Categorías especiales de datos personales:** Se considerarán categorías especiales de datos personales, los siguientes:
- a) Datos sensibles; b) Datos de niñas, niños y adolescentes; c) Datos de salud; y, d) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.
- **Consentimiento:** Manifestación de la voluntad libre, específica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos.
- **Dato biométrico:** Dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros.
- **Dato genético:** Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo.
- **Dato personal:** Dato que identifica o hace identificable a una persona natural, directa o indirectamente.
- **Datos personales crediticios:** Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera.
- **Datos relativos a:** etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos, datos relativos a las personas apátridas y refugiados que requieren protección internacional, y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.
- **Datos relativos a la salud:** datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

- **Datos sensibles:** Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.
- **Delegado de protección de datos:** Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos.
- **Destinatario:** Persona natural o jurídica que ha sido comunicada con datos personales.
- **Elaboración de perfiles:** Todo tratamiento de datos personales que permite evaluar, analizar o predecir aspectos de una persona natural para determinar comportamientos o estándares relativos a: rendimiento profesional, situación económica, salud, preferencias personales, intereses, Habilidad, ubicación, movimiento físico de una persona, entre otros.
- **Encargado del tratamiento de datos personales:** Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.
- **Entidad Certificadora:** Entidad reconocida por la Autoridad de Protección de Datos Personales, que podrá, de manera no exclusiva, proporcionar certificaciones en materia de protección de datos personales.
- **Fuente accesible al público:** Bases de datos que pueden ser consultadas por cualquier persona, cuyo acceso es público, incondicional y generalizado.
- **Integrantes del sistema de protección de datos personales:**
    1. Titular;
    2. Responsable del tratamiento;
    3. Encargado del tratamiento;
    4. Destinatario;
    5. Autoridad de Protección de Datos Personales; y,
    6. Delegado de protección de datos personales.
- **LOPDP.** Ley Orgánica de Protección de Datos Personales
- **PPGA.** Best Doctors, S.A. Empresa de medicina prepagada.
- **Responsable de tratamiento de datos personales:** persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales.
- **Sellos de protección de datos personales:** Acreditación que otorga la entidad certificadora al responsable o al encargado del tratamiento de datos personales, de haber implementado mejores prácticas en sus procesos, con el objetivo de promover la confianza del titular, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.
- **Seudonimización:** Tratamiento de datos personales de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional, figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.
- **Titular:** Persona natural cuyos datos son objeto de tratamiento.
- **Transferencia o comunicación:** Manifestación, declaración, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una

persona distinta al titular, responsable o encargado del tratamiento de datos personales. Los datos personales que comuniquen deben ser exactos, completos y actualizados.

- **Tratamiento:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.
- **Vulneración de la seguridad de los datos personales:** Incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales.

Control de Cambios				
Versión	**Fecha de Actualización**	**Tipo de Cambio**	**Descripción de la modificación**	**Área solicitante del cambio**
1	**Mayo 2023**	**A**	**Elaboración de documento**	**Compliance**

(*) A: Agregar – M: Modificar – E: Eliminar

Control de Cambios