



# PLAN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

## Superintendencia de Protección de Datos Personales

| FECHA DE ELABORACIÓN Y/O ACTUALIZACIÓN                                                                            | 12/may/2025                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RESPONSABILIDAD DE FIRMA / NOMBRE / CARGO                                                                         | FIRMA                                                                                                                                                                                                                                            |
| <b>Elaborado por:</b><br>Karina Alexandra Fiallos Cortázar<br>Especialista de Gestión Estratégica y Planificación | KARINA<br>ALEXANDRA<br>FIALLOS<br>CORTAZAR<br><br>Firmado digitalmente<br>por KARINA ALEXANDRA<br>FIALLOS CORTAZAR<br>Fecha: 2025.05.12<br>09:57:10 -05'00' |
| <b>Revisado y Aprobado por:</b><br>Fabrizio Peralta-Díaz<br>Superintendente de Protección de Datos Personales     | <br>Firmado electrónicamente por:<br><b>FABRIZIO ROBERTO<br/>PERALTA DIAZ</b><br>Validar únicamente con FirmaEC                                             |



**Superintendencia de Protección de Datos Personales**

Avda. Río Amazonas entre Pereira y Unión Nacional de Periodistas  
Edificio Plataforma Gubernamental de Gestión Financiera  
Bloque Amarillo Piso 5  
PBX: + (593 2) 470 0047  
Código Postal: 170507  
[www.spdp.gob.ec](http://www.spdp.gob.ec)

**Autoridades:**

Fabrizio Peralta-Díaz, Superintendente de Protección de Datos Personales.  
Manuel Jacho Chávez, Intendente General de Regulación.  
René Orbe Pacheco, Intendente General de Control y Sanción.  
Luis Enríquez Álvarez, Intendente General de Innovación Tecnológica.

**Equipo de redacción y coautores:**

Karina Fiallos Cortázar  
Rafael Tupiza Morla  
Isaac Delgado Vélez

**Equipo de colaboradores:**

Santiago Ludeña Ramírez  
Vanessa Hervás Novoa  
Susan Del Pozo Larrea

Quito, D. M., mayo del 2025



**Contenido**

|      |                                                                                                                                 |    |
|------|---------------------------------------------------------------------------------------------------------------------------------|----|
| 1.   | INTRODUCCIÓN.....                                                                                                               | 4  |
| 2.   | MARCO NORMATIVO .....                                                                                                           | 4  |
| 3.   | OBJETIVOS.....                                                                                                                  | 6  |
| 3.1. | Objetivo General.....                                                                                                           | 6  |
| 3.2. | Objetivos específicos .....                                                                                                     | 6  |
| 4.   | ALCANCE .....                                                                                                                   | 6  |
| 5.   | DIAGNÓSTICO.....                                                                                                                | 7  |
| 5.1. | Contexto general.....                                                                                                           | 7  |
| 5.2. | Identificación de la problemática .....                                                                                         | 9  |
| 5.3. | Identificación de oportunidades desarrollo.....                                                                                 | 11 |
| 5.4. | Identificación de necesidades de política y/o plan nacional.....                                                                | 12 |
| 6.   | PROPUESTA .....                                                                                                                 | 13 |
| 6.1. | Alternativas de solución. ....                                                                                                  | 13 |
| 6.2. | Priorización de alternativas .....                                                                                              | 13 |
| 6.3. | IDENTIFICACIÓN DE EJES ESTRATÉGICOS.....                                                                                        | 15 |
| 6.4. | Proyectos y Presupuesto Referencial.....                                                                                        | 21 |
| 7.   | VINCULACIÓN DEL PLAN NACIONAL DE PROTECCIÓN DE DATOS<br>PERSONALES CON AGENDA ODS 2030 Y EL PLAN NACIONAL DE<br>DESARROLLO..... | 21 |
| 7.1. | Agenda Objetivos de Desarrollo Sostenible 2030:.....                                                                            | 21 |
| 7.2. | Articulación con el Plan Nacional de Desarrollo 2024 - 2025 .....                                                               | 22 |
| 8.   | CONCLUSIONES Y RECOMENDACIONES .....                                                                                            | 22 |
| 9.   | GLOSARIO .....                                                                                                                  | 23 |
| 10.  | REFERENCIAS .....                                                                                                               | 24 |
| 11.  | ANEXOS.....                                                                                                                     | 25 |

**ÍNDICE DE ILUSTRACIONES**

|                                                                                                                   |    |
|-------------------------------------------------------------------------------------------------------------------|----|
| <i>Ilustración 1 Principales indicadores de la Encuesta de Percepción sobre Protección de Datos Personales. .</i> | 10 |
| <i>Ilustración 2 Imagen creada por inteligencia artificial por los autores PNPDP .....</i>                        | 15 |
| <i>Ilustración 3 Imagen creada por inteligencia artificial por los autores – Objetivo Estratégico #1 .....</i>    | 15 |
| <i>Ilustración 4 Imagen creada por inteligencia artificial por los autores - Objetivo Estratégico #2 .....</i>    | 17 |
| <i>Ilustración 5 Imagen creada por inteligencia artificial por los autores - Objetivo Estratégico #3 .....</i>    | 19 |

**ÍNDICE DE TABLAS**

|                                                                                                   |    |
|---------------------------------------------------------------------------------------------------|----|
| <i>Tabla 1 Priorización de alternativas de solución.....</i>                                      | 14 |
| <i>Tabla 2 Metas e indicadores – OE1 .....</i>                                                    | 16 |
| <i>Tabla 3 Metas e indicadores – OE2 .....</i>                                                    | 18 |
| <i>Tabla 4 Metas e indicadores – OE3 .....</i>                                                    | 20 |
| <i>Tabla 5 Presupuesto referencial por año .....</i>                                              | 21 |
| <i>Tabla 6 Alineación del PNPDP con la Agenda 2030.....</i>                                       | 21 |
| <i>Tabla 7 Articulación de los Objetivos del Plan PDP con objetivos y políticas del PND .....</i> | 22 |



## **1. INTRODUCCIÓN**

La protección de los datos personales se vuelve un pilar esencial para construir una sociedad digital ética, segura y centrada en la defensa de los derechos humanos en la era digital. Desde la segunda mitad del siglo XX, el desarrollo tecnológico ha planteado importantes desafíos en relación a la privacidad y la administración ética de la información. En América Latina, el avance es significativo. El Ecuador se sumó a esta tendencia mediante la promulgación de la Ley Orgánica de Protección de Datos Personales (LOPD) en 2021.

A pesar de este importante paso, el país enfrenta desafíos de carácter estructural-cultural que dificultan la implementación efectiva de la normativa, entre ellos: la baja conciencia ciudadana; la falta de formación en materia de protección de datos; la débil infraestructura tecnológica; y una débil institucionalidad. Estos desafíos, sumados a la rápida evolución digital y a la demanda de transparencia y seguridad, exigen una respuesta integral, articulada y sostenida.

El Plan Nacional de Protección Datos Personales tiene como finalidad sentar las bases para un entorno digital seguro y confiable, en el que se garantice el respeto a la privacidad y se promueva una cultura en torno a aquella, mediante la adecuada protección de los datos personales. Con tales premisas, se estructuran tres ejes fundamentales:

1. Fortalecimiento de la gobernanza digital;
2. Universalización del derecho a la protección de datos y promoción de la cultura ciudadana; y,
3. Innovación y vigilancia digital para un ecosistema nacional seguro.

Con una visión integral de mediano y largo plazo, mediante una colaboración activa entre el Estado, la sociedad civil, el sector privado y la academia, será posible consolidar un sistema de protección de datos que garantice la confianza, la inclusión y el desarrollo sostenible del país en la era digital.

## **2. MARCO NORMATIVO**

Los instrumentos internacionales en materia de protección, privacidad y seguridad de los datos personales, así como diversas organizaciones tales como la Organización de las Naciones Unidas (ONU), el Consejo de Europa, la Unión Europea (UE), la Organización para la Cooperación y el Desarrollo Económico (OCDE) y la Organización de los Estados Americanos (OEA), han remarcado la importancia de garantizar la seguridad de los datos y proteger los derechos fundamentales en la era digital.

La ONU ha sido una de las entidades internacionales más influyentes en la protección de los derechos humanos, entre los que se incluye el derecho a la privacidad. Así, en el artículo 12 de la *Declaración Universal de los Derechos Humanos*, del 10 de diciembre de 1948, proclamó que “[n]adie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”. Posteriormente, y a través del artículo 17 del *Pacto Internacional de Derechos Civiles y Políticos*, del 16 de diciembre de 1966, la ONU reiteró, en términos similares, el precepto antes citado; y, luego, mediante su resolución 45/95, del 14 de diciembre de 1990, aprobó los *principios rectores sobre la reglamentación de los ficheros computarizados de datos personales*, que fueron sugeridos para que los Estados las tuviesen presentes en sus leyes y reglamentos, tales como los de licitud y



lealtad; el de exactitud; el de finalidad; los de acceso y no discriminación de la persona interesada, entre otros<sup>1</sup>.

El Consejo de Europa ha sido, también, un actor clave en la regulación del tratamiento de datos personales, mediante la celebración un tratado internacional vinculante que establece las bases para la protección de datos personales a nivel europeo<sup>2</sup>, a través de normas que deben ser respetadas por los Estados miembros; y que adhiere a los principios que guían el tratamiento de los datos personales.

El RGPD de la UE<sup>3</sup> representa el estándar más avanzado en el ámbito de la protección de datos personales y establece un amplio marco normativo para los países miembros, así como para las empresas y organizaciones que tratan datos de ciudadanos europeos. Este reglamento ha servido como un modelo normativo para muchos países, entre ellos, el Ecuador.

La OCDE fomenta la protección de la privacidad y la transacción entre países de los datos personales, además de promover principios como la responsabilidad y la seguridad de los datos personales<sup>4</sup>. Estas directrices sientan las bases de una cooperación internacional para asegurar que los datos puedan circular entre países sin que ello represente riesgo.

La OEA ha abordado el tema de la privacidad y la protección de datos personales en el contexto de los derechos humanos<sup>5</sup>, para promover que los países miembros protejan los derechos de los titulares respecto de sus datos<sup>6</sup>. También ha recomendado a los Estados desarrollar políticas y marcos normativos que respeten la privacidad de los ciudadanos, además de impulsar la cooperación intergubernamental en materia de protección de datos personales y el intercambio seguro de información.

La CRE establece el derecho a la protección de datos personales como uno de carácter fundamental, para así garantizar la privacidad de las personas y el derecho a controlar su información. El reconocimiento de este derecho constitucional ha implicado para el Estado el deber de expedir la legislación correspondiente, crear la institucionalidad para garantizar su cumplimiento e implementar mecanismos de seguridad y transparencia<sup>7</sup>.

La puesta en marcha de dicha institucionalidad se materializa a través de la creación de la Superintendencia de Protección de Datos Personales, que, como organismo técnico de vigilancia, auditoría y control, detenta un rol protagónico en el efectivo cumplimiento de los derechos de los titulares de la información<sup>8</sup>.

La LOPDP, a su vez, instituye una serie de principios que guían el tratamiento de los datos personales. Estos principios son los que los pilares sobre los cuales se debe construir el Plan Nacional de Protección de Datos Personales, para procurar que el tratamiento debido de los datos de las personas se realice de conformidad con las mejores prácticas internacionales y con los estándares de derechos humanos, además de promover la necesidad de que la SPDP

---

<sup>1</sup> Otro documento relevante puede hallarse en el Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos que se titula *El derecho a la privacidad en la era digital*, distribuido el 30 de junio del 2014 y que fue preparado en virtud del pedido formulado por la Asamblea General de la ONU a través de la resolución 68/167, del 18 de diciembre del 2013.

<sup>2</sup> Convenio 108, de 1981. A este instrumento se le añadió un Protocolo Adicional, del 2001, conocido como *el 108+*. No obstante, el 18 de mayo del 2018, el Comité de Ministros del Consejo adoptó un nuevo protocolo, que actualizó al Convenio 108.

<sup>3</sup> Reglamento General de Protección de Datos, vigente desde el 2018.

<sup>4</sup> Recomendación del 2013.

<sup>5</sup> Convención Interamericana sobre la Protección de los Derechos Humanos.

<sup>6</sup> Carta Democrática Interamericana.

<sup>7</sup> CRE, artículo 66, numeral 19.

<sup>8</sup> CRE, artículo 213.



actúe de manera independiente, imparcial y autónoma para asegurar el ejercicio efectivo del derecho a la protección de datos personales<sup>9</sup>.

En suma, el desarrollo y ejecución de un Plan Nacional de Protección de Datos Personales no solo que podría reforzar el cumplimiento de la CRE, la LOPDP, su Reglamento General, los instrumentos internacionales ratificados por el Ecuador y las demás disposiciones aplicables, sino que también constituye una estrategia para favorecer el desarrollo del Ecuador en el entorno digital, en observancia de los principios rectores en el tratamiento de datos personales y a través de la promoción un tratamiento adecuado en todos los niveles de los sectores público y privado.

### 3. OBJETIVOS

#### 3.1. Objetivo General

Desarrollar e implementar un plan nacional que promueva la confianza en los servicios digitales, coadyuve a garantizar la protección de los derechos de los ciudadanos y fortalezca la institucionalidad en el ámbito de la privacidad y seguridad de los datos.

#### 3.2. Objetivos específicos

- Promover una cultura de protección de datos mediante capacitación y sensibilización en instituciones públicas y privadas.
- Generar conciencia y formación ciudadana para procurar que conozcan sus derechos y obligaciones en materia de protección de datos personales.
- Facilitar la integración del Ecuador en la lista de países con nivel adecuado de tratamiento de datos, para que se lo reconozca como un país confiable para el intercambio de información digital a nivel global.

### 4. ALCANCE

El Plan busca establecer una estrategia para fortalecer el tratamiento y la protección de datos personales en el Ecuador, que garantice su tratamiento adecuado que se adecue a los desarrollos tecnológicos. Con implementación se pretende generar un entorno digital seguro, que proteja los derechos de los ecuatorianos en un entorno tecnológico de constante crecimiento.

El Plan se enmarca en una estrategia de gobernanza digital, que impulse la confianza en el uso de servicios digitales y procure un equilibrio entre la innovación tecnológica y los derechos de los ciudadanos. Se aspira a que su implementación pueda contribuir a fortalecer la institucionalidad en materia de protección de datos, y que pueda ser capaz de impulsar un entorno digital seguro y respetuoso.

El alcance del Plan no solo se limita a la aplicación de los principios y las normativas establecidas, sino que promueve la consolidación de una cultura de protección de datos a través de la sensibilización y formación de los integrantes del sistema de protección de datos personales. Al respecto, merece relieves que, de acuerdo con la información del Registro Estadístico de Empresas (REEM 2023) del Instituto Nacional de Estadística y Censos (INEC), se estima que el número de sujetos regulados, en el sector privado, asciende aproximadamente a **un millón ciento sesenta y siete mil ciento una (1'167.101)** empresas, considerando el sistema de información de empresas del país y que está estructurada a partir de registros administrativos. Entre las instituciones que participan constan el SRI, el IEISS, Ministerio de

---

<sup>9</sup> LOPDP, artículo 10.



Educación, el Ministerio de Turismo, la Superintendencia de Compañías, Valores y Seguros, la Superintendencia de Bancos, la Superintendencia de Economía Popular y Solidaria y la Encuesta Estructural Empresarial del INEC<sup>10</sup>.

Adicionalmente, por la información recabada por la SPDP, se tiene que los sujetos regulados del sector público son: cinco (5) entidades entre bancos e instituciones financieras públicas y tres mil ciento cuarenta y una (3.141) entidades consideradas por el Presupuesto General del Estado, es decir, aquellas pertenecientes a las cinco funciones del Estado (Ejecutiva, Legislativa, Judicial, Electoral y de Transparencia y Control Social).

Por otro lado, el Plan busca alinear al Ecuador con estándares internacionales para favorecer la competitividad del país y su integración en lista de países con nivel adecuado de tratamiento de datos. Por ende, su implementación fortalecerá la confianza en el uso debido y seguro de los datos personales, que favorezca y dinamice un desarrollo tecnológico responsable y ético en beneficio de los ecuatorianos.

## **5. DIAGNÓSTICO**

### **5.1. Contexto general**

La protección de datos personales se remonta a mediados del siglo XX, cuando el avance tecnológico y la expansión del uso de computadoras plantearon inquietudes en torno a la privacidad de las personas. En 1970, Alemania (concretamente, el *land* alemán de Hesse) fue pionera en establecer la primera ley de protección de datos; ejemplo que, luego, fue seguido por otros países europeos.

Con el pasar de los años, el desarrollo del internet y las tecnologías digitales transformaron drásticamente la forma en que se recopilan, almacenan y procesan los datos personales. Esto llevó a la adopción de normativas más estrictas en varios países del mundo, entre las que destaca el RGPD de la UE del 2016, que marcó un hito universal en la regulación de la privacidad.

En América Latina, la protección de datos personales ha ido cobrando importancia en las últimas dos décadas. Países como Argentina, Uruguay, Colombia, México, Brasil, Paraguay, Panamá, Perú y Chile han promulgado leyes específicas que regulan el tratamiento de datos personales. La chilena Ley N° 19.628, sobre protección de la vida privada, fue la primera de la región (1999); y, luego, le siguió la Ley N° 25.326, de Protección de los Datos Personales, promulgada en la Argentina (2000), que fue la primera que se basó en el molde normativo dado por la Directiva (UE) 95/46/CE.

A nivel regional, la Comisión Económica para América Latina y el Caribe (CEPAL) ha promovido iniciativas para fortalecer la protección de datos y fomentar un enfoque coordinado entre los países de la región.

A nivel internacional, la protección de datos personales se ha convertido en un tema central en el ámbito de los derechos humanos y la gobernanza digital. La progresiva inquietud por la privacidad ha llevado a que diferentes entidades, como la Organización

---

<sup>10</sup> Estas estimaciones son meramente referenciales, dado que la LOPDP tiene como ámbito de aplicación material “al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior” (LOPDP, artículo 2). La LOPDP no establece, pues, un listado exhaustivo de sujetos regulados o controlados, sino que se ocupa de que los datos personales, sin importar quién los utilice y con qué fines, sean tratados de acuerdo con los principios instituidos en la legislación. En otras palabras, todo aquel que trate datos personales está potencialmente sujeto al control, vigilancia y sanción de la SPDP, salvo los casos en los que la propia LOPDP ha establecido puntuales excepciones.



de las Naciones Unidas y el Consejo de Europa, desarrollen marcos normativos y directrices que promueven el respeto a la privacidad y la protección de datos.

Además del RGPD, otros tratados y acuerdos, como el ya citado Convenio 108 del Consejo de Europa, han influido en la legislación de protección de datos de diversos países. En el ámbito global, la colaboración entre naciones se ha intensificado para abordar desafíos comunes relacionados con el intercambio de datos y la ciberseguridad, lo que ha llevado a la creación de estándares internacionales a fin de garantizar la protección efectiva de los datos personales.

El Ecuador se encuentra en un momento determinante en su proceso de transformación digital. El uso de tecnologías de la información y comunicación se encuentra en constante evolución, lo que facilita el acceso a una gran cantidad de datos personales por parte de entidades públicas y privadas, lo que a su vez ha generado inquietud sobre la protección de la privacidad y la seguridad de la información. Sin embargo, a pesar de los indiscutibles avances, el país enfrenta desafíos en la gestión y protección de datos.

La LOPDP, promulgada en el 2021, representa un paso significativo en la regulación del tratamiento de datos en nuestro país. La ley establece derechos fundamentales para los titulares de datos, como los de información, acceso, rectificación, actualización, eliminación, oposición, entre otros.

Es importante reconocer que la implementación de la normativa ha sido desigual: muchas organizaciones, tanto del sector público como del privado, carecen de políticas claras y procedimientos efectivos para cumplir con las exigencias legales; ello sin dejar de lado que, a través de la SPDP, el país se encuentra desarrollando normativa secundaria alineada con estándares internacionales.

Un aspecto fundamental que complica la situación es la baja conciencia sobre la protección de datos de los ciudadanos. La mayor parte de la población no está informada sobre sus derechos, ni sobre cómo proteger su información personal. Esto se debe, en parte, a la falta de campañas educativas efectivas que sensibilicen sobre la importancia de la privacidad en la era digital. En el ámbito privado, muchas organizaciones no consideran prioritario invertir en la educación de sus empleados sobre la gestión adecuada de datos, lo que contribuye a la perpetuación de prácticas inadecuadas en el manejo de los datos de sus clientes, trabajadores, proveedores, entre otros.

La sensibilización respecto a los temas de protección de datos es esencial para el manejo adecuado de la información. Sin embargo, el Ecuador enfrenta retos significativos en este ámbito. Las iniciativas de capacitación y promoción son escasas y, a menudo, carecen de la especialización necesaria para abordar las particularidades de diferentes sectores. Esto deriva en una falta de preparación para gestionar datos, particularmente los de carácter sensible, y para responder adecuadamente a incidentes de seguridad. La formación limitada deja a las entidades expuestas a vulneraciones de seguridad que podrían evitarse con un personal adecuadamente capacitado.

Es imperativa la adopción de tecnologías avanzadas, lo que plantea riesgos adicionales en términos de protección de datos, dado que muchas organizaciones carecen de la infraestructura adecuada (para salvaguardar la información personal, lo que las hace susceptibles a ciberataques y brechas de datos) les faltan protocolos de ciberseguridad y no ejecutan auditorías regulares, lo que aumenta la vulnerabilidad de los datos y, de esta forma, los ciudadanos quedan expuestos a conductas abusivas y al mal uso de su información.

La SPDP, aunque es el ente encargado de supervisar y regular el cumplimiento de la normativa, enfrenta múltiples retos: la falta de recursos y de personal limita su capacidad



para llevar a cabo auditorías efectivas y supervisar a las entidades que manejan datos personales. Esta situación se agrava por la falta de un sistema legal que permita sanciones efectivas, es decir, no condicionadas al establecimiento de medidas correctivas, lo que puede llevar a las organizaciones a desestimar la importancia de cumplir con la ley.

El contexto internacional también influye en la situación de la protección de datos en el Ecuador. La globalización y la interconexión digital exigen que los países se alineen con estándares internacionales para facilitar el comercio y proteger a sus ciudadanos. La presión de organismos internacionales y la creciente demanda de transparencia y responsabilidad en el manejo de datos personales, hacen que sea urgente que el Ecuador avance en la implementación de políticas efectivas y en la modernización de un marco normativo capaz de acompañar el ritmo de los avances tecnológicos.

Es determinante admitir que los problemas de protección de datos no solo afectan a los individuos, sino que también tienen consecuencias para el desarrollo económico y social del país. La desconfianza en el manejo de datos podría desincentivar el uso de servicios digitales, limitar la innovación y obstaculizar el crecimiento de la economía digital. Consecuentemente, las violaciones a la privacidad pueden tener un impacto desproporcionado en grupos vulnerables, además de exacerbar las desigualdades sociales y limitar el acceso a oportunidades.

La situación de la protección de datos personales en el Ecuador es compleja y multifacética. Un marco normativo aún en desarrollo, combinado con baja conciencia pública, falta de capacitación y riesgos tecnológicos, crea un entorno vulnerable para la privacidad de los ciudadanos. Abordar estos desafíos es crucial para garantizar la protección efectiva de los datos personales y fomentar un entorno digital seguro y confiable.

La colaboración entre el Estado, las empresas, la academia y la sociedad civil será fundamental para avanzar en esta área y construir un futuro en el que la privacidad y la seguridad de la información sean una prioridad para todos, sin descuidar la infraestructura tecnológica que permita acercar los servicios a los ciudadanos, para asegurar la optimización de los recursos y la sostenibilidad de las acciones ejecutadas.

## **5.2. Identificación de la problemática**

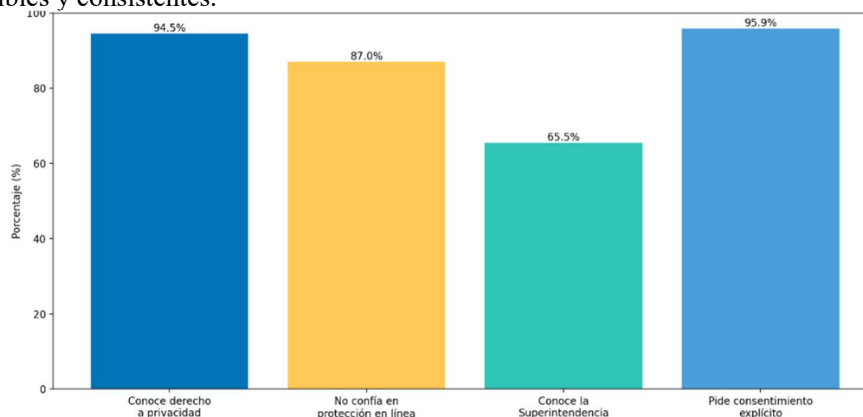
Basados en los resultados de la Encuesta de Percepción Ciudadana sobre Protección de Datos Personales, los encuestados, en su mayoría, afirman estar familiarizados con el derecho a la privacidad; sin embargo, en la práctica, no se sienten seguros de que su información esté debidamente protegida por las entidades públicas y privadas. Es decir, la percepción de inseguridad sugiere una brecha entre la existencia formal de los derechos y la garantía efectiva de aquellos.

Por otro lado, los resultados de la tabulación de la encuesta identifican que la población no tiene claridad sobre cómo sus datos están siendo utilizados, lo que refleja falta de transparencia y educación digital.

Esto representa, un desafío urgente para la construcción de políticas públicas en el marco de la protección de datos personales, lo que torna necesario transformar el *conocimiento pasivo* en *confianza activa*, con estrategias que fortalezcan la institucionalidad y, a la par, promuevan la capacitación accesible para generar prácticas



visibles y consistentes.



**Ilustración 1** Principales indicadores de la Encuesta de Percepción sobre Protección de Datos Personales.  
**Fuente:** Resultados de la Encuesta de Percepción ejecutado por la SPDP (abril-2025)

Con los antecedentes expuestos en el apartado anterior, y gracias a la información generada mediante encuestas a la ciudadanía y entrevistas realizadas a diferentes expertos de la protección de datos, podemos identificar algunos de los diferentes problemas que se generan en el ámbito de la protección de datos en el Ecuador, que son los que se enumera a continuación:

1. **Brecha entre la ley y la institucionalidad:** La LOPDP no se está aplicando de manera efectiva en sectores público y privado. La no implementación adecuada de la normativa, así como las practicas inadecuadas en materia de protección de datos, se traduce en un aumento del riesgo de violaciones a la privacidad.
2. **Desconocimiento de derechos:** La población, en general, carece de información sobre sus derechos en relación con la protección de sus datos personales, lo que limita su capacidad para ejercer sus derechos. Ello ocasiona que los ciudadanos se encuentren en una posición de vulnerabilidad frente al manejo de sus datos.
3. **Falta de conocimiento:** Las organizaciones no cuentan con programas adecuados de formación en manejo de datos personales, lo que ocasiona que las entidades cometan errores y e incurran en negligencia en temas de seguridad.
4. **Baja conciencia pública:** Existe poca sensibilización sobre la importancia de la protección de datos en la era digital. La falta de campañas informativas y educativas impide que la ciudadanía comprenda los riesgos asociados con la administración de su información personal, lo que ocasiona una actitud pasiva frente a la protección de sus datos.
5. **Riesgos de ciberseguridad:** La falta de sistemas de seguridad robustos, actualizaciones periódicas y protocolos frente a incidentes, ocasiona que las entidades estén expuestas a ataques que comprometan información sensible.
6. **Vulnerabilidad o brechas de seguridad:** La falta de protocolos de seguridad aumenta el riesgo de incidentes que comprometen la privacidad de la información. Sin medidas adecuadas para proteger los datos, se incrementa la probabilidad de sufrir brechas de seguridad que puedan ocasionar la exposición o sustracción de información personal.



7. **Recursos limitados para la supervisión:** La SPDP enfrenta limitaciones en los recursos, sobre todo presupuestarios y de personal, para poder ejercer su función de supervisión y control, lo que limita su capacidad para ejecutar inspecciones y auditorías, así como para diligenciar procesos administrativos sancionatorios.
8. **Tratamiento inadecuado de datos:** El uso de tecnologías como Big Data e inteligencia artificial se realiza sin supervisión adecuada, lo que puede llevar a decisiones discriminatorias y tratamiento inadecuado de la información personal.
9. **Falta de alianzas internacionales:** La escasa alineación con estándares internacionales dificulta la cooperación en temas de protección de datos y la confianza en el manejo de información personal. La ausencia de colaboración con organismos internacionales limita el acceso a recursos, conocimientos y experiencias que fortalezcan su implementación en el país.

A partir de lo expuesto, podemos concluir que la problemática identificada en materia de protección de datos personales se estructura de la siguiente manera:

*El tratamiento de datos en el Ecuador no cumple con la normativa básica requerida ni se alinea con estándares internacionales. Esto se agrava por la falta de recursos del recién creado ente de control, así como por la escasa comprensión sobre los derechos establecidos en la LOPDP, la falta de capacitación y la limitada conciencia pública.*

*Además, los riesgos de ciberseguridad aumentan ante el acelerado avance tecnológico. Como resultado, no se garantiza adecuadamente el derecho fundamental a la protección de los datos personales, tal como lo establece la Constitución de la República del Ecuador y los principios de derechos humanos.*

### 5.3. Identificación de oportunidades desarrollo

1. **Eficiente implementación del marco regulatorio de PDP:** Es necesario desarrollar estrategias robustas para asegurar la aplicación efectiva de la LOPDP tanto en el sector público como en el privado; estrategias que impliquen la creación de marcos normativos específicos que garanticen la transparencia y la rendición de cuentas en el manejo de los datos.
2. **Concientización sobre derechos:** Se requiere desarrollar una campaña integral de sensibilización y educación dirigida a la población. Esta campaña debe incluir talleres, seminarios, recursos digitales que expliquen de manera accesible, a todos los estratos de la sociedad, cuáles son los derechos de las personas y las obligaciones de las organizaciones que tratan datos personales.
3. **Capacitación organizacional:** Es primordial establecer programas de formación adecuados para que las organizaciones manejen correctamente los datos personales de las personas. Estos programas deben considerar módulos sobre legislación vigente, mejores prácticas en la gestión de datos, abordajes en situaciones de riesgo o incumplimientos y seguridad de la información.
4. **Aumento de la conciencia pública:** Es necesario promover una mayor sensibilización sobre la importancia de la protección de datos en el contexto digital actual, mediante campañas masivas en medios públicos.



5. **Fortalecimiento de la ciberseguridad:** Se requiere incentivar a las organizaciones para que inviertan en infraestructura y tecnologías que protejan adecuadamente los datos personales, mediante la implementación de cifrado, firewalls avanzados y adopción de estándares de seguridad reconocidos internacionalmente, que permitan una mayor protección contra accesos no autorizados y ciberataques.
6. **Establecimiento de protocolos de seguridad:** Es imperativo implementar protocolos claros y específicos de seguridad, que deberán contemplar procedimientos de recolección, almacenamiento y eliminación de datos, con el afán de reducir el riesgo de brechas de seguridad y así reducir el riesgo de incidentes.
7. **Recursos para supervisión y control:** La SPDP requiere recursos adicionales, tanto presupuestarios como humanos, para desempeñar su función de manera efectiva, lo que permitirá la contratación de personal técnicamente capacitado para reforzar los procesos sustantivos, así como la generación de herramientas tecnológicas que faciliten la supervisión de la implementación de la normativa.
8. **Supervisión del tratamiento de datos:** Es necesario establecer mecanismos de supervisión para el uso de nuevas tecnologías, que eviten decisiones discriminatorias que puedan surgir del análisis de los datos. Esto implicaría una evaluación periódica de los algoritmos utilizados y el establecimiento de auditorías que aseguren la equidad en el tratamiento de la información.
9. **Fortalecimiento de alianzas internacionales:** Se debe procurar el establecimiento de vínculos de cooperación con autoridades de protección de datos extranjeras y con entidades internacionales, para alinearse con estándares globales en protección de datos que nos permitan acceder a mayores recursos, conocimientos y tecnologías, así como también compartir conocimientos y buenas prácticas con otros países.

#### **5.4. Identificación de necesidades de política y/o plan nacional**

La CRE, artículo 66, numeral 19, les reconoce y garantiza a las personas el “derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección”. En consecuencia, y por mandato de la citada norma constitucional, “[l]a recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley”.

Sobre la base de la citada norma fundamental se expidió la LOPDP, que establece como principios los de juridicidad, lealtad, transparencia, finalidad, pertinencia y minimización, proporcionalidad, confidencialidad, calidad y exactitud, conservación, seguridad, responsabilidad proactiva y demostrada, aplicación favorable al titular e independencia de control.

Adicionalmente, la citada norma de rango legal instituye, a favor de los titulares, un amplio haz de derechos que pueden directamente ejercer contra los responsables y encargados del tratamiento, quienes, a su vez, están obligados a tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas para prevenir, impedir, reducir, mitigar y controlar los riesgos detectados y las potenciales vulneraciones que



podrían sobrevenir sobre los datos personales; medidas que deben adoptarse, precisamente, sobre la base del aludido principio de responsabilidad proactiva.

Sin embargo, el inadecuado tratamiento de datos personales representa un **problema estructural en el país**. La carencia detectada no solo vulnera la privacidad de los ciudadanos, sino que también socava la confianza en las instituciones y organizaciones por el indebido manejo de la información personal, lo que puede traer consecuencias graves en un contexto donde la protección de datos es fundamental, a fin de generar confianza en todos los sectores de la sociedad.

Por lo antes expuesto, es imperativo contar con una perspectiva multidimensional ante la necesidad de generar políticas públicas en materia de protección de datos personales, considerando que se conjugan elementos sociales, políticos, legales, multiculturales y económicos; así debe también contarse con análisis detallados de las necesidades locales que permitan identificar los mecanismos pertinentes en los diferentes niveles territoriales, a fin de acercar el derecho a todos los ciudadanos del territorio ecuatoriano de manera integral.

## 6. PROPUESTA

### 6.1. Alternativas de solución.

Una vez identificada la problemática y sus causas asociadas, es fundamental plantear alternativas de solución viables y estratégicas que permitan abordar, de manera efectiva, las oportunidades de desarrollo.

Con estas propuestas se busca garantizar el derecho a la protección de datos personales en el Ecuador, desde un enfoque integral que combine aspectos técnicos, financieros, políticos, sociales, legales e institucionales.

El diseño de las alternativas parte del reconocimiento de las brechas existentes en la aplicación de la LOPDP, así como de la necesidad de fortalecer las capacidades del Estado, las organizaciones y la ciudadanía para asegurar un entorno digital justo, seguro y transparente.

A continuación, se presentan las principales alternativas formuladas:

- Proveer de recursos a la SPDP.
- Diseñar y ejecutar campañas de sensibilización.
- Alinear la normativa ecuatoriana con estándares internacionales.
- Regular el desarrollo tecnológico con enfoque en derechos.
- Desarrollar herramientas tecnológicas de supervisión.
- Capacitar e incorporar personal técnico.
- Establecer procedimientos claros para el tratamiento de datos.
- Fomentar inversión en ciberseguridad con enfoque en la protección de datos.

### 6.2. Priorización de alternativas

Una vez identificadas las alternativas de solución, se procedió a su priorización mediante el método del Ábaco de François Régnier.

Para ello, se definieron criterios de evaluación relacionados con viabilidad técnica, financiera, política, social, legal e institucional. El análisis se realiza asignando puntuaciones en la escala del 1 al 5, donde 5 representa el mayor nivel de impacto o

# SUPERINTENDENCIA DE PROTECCIÓN DE DATOS PERSONALES



relevancia según cada criterio. El resultado de este análisis técnico se muestra en la siguiente tabla:

**Tabla 1** Priorización de alternativas de solución

| Alternativas                                    | Técnica | Financiera | Política | Social | Legal | Institucional | Total |
|-------------------------------------------------|---------|------------|----------|--------|-------|---------------|-------|
| Recursos SPDP                                   | 5       | 5          | 4        | 4      | 5     | 5             | 28    |
| Procedimientos para tratamiento                 | 5       | 4          | 4        | 4      | 5     | 5             | 27    |
| Campañas de sensibilización                     | 4       | 5          | 4        | 5      | 4     | 4             | 26    |
| Capacitación técnica                            | 4       | 4          | 4        | 4      | 4     | 5             | 25    |
| Herramientas de supervisión                     | 4       | 3          | 2        | 3      | 5     | 4             | 21    |
| Inversión en ciberseguridad para la PDP         | 4       | 3          | 3        | 4      | 4     | 4             | 21    |
| Normativa alineada a estándares internacionales | 4       | 3          | 2        | 3      | 5     | 3             | 20    |
| Fomentar inversión en tecnología                | 3       | 2          | 2        | 2      | 4     | 4             | 17    |

**Elaboración:** Superintendencia de Protección de Datos Personales

El análisis muestra que el fortalecimiento institucional del ente regulador es una acción prioritaria para garantizar un ecosistema robusto en la protección de datos personales, dado que permitirá gestionar la protección de datos personales de forma técnica y jurídica, tanto a nivel institucional como interinstitucional, seguido por su impacto inmediato y factibilidad, a través de la implementación de procedimientos para el tratamiento de datos el desarrollo de campañas de sensibilización ciudadana y la capacitación técnica a los responsables, lo que demuestra que el enfoque inicial debe centrarse en medidas de bajo costo, pero con alto impacto estructural y social.

En contraste, deberán ejecutarse acciones como la alineación normativa con estándares internacionales y la regulación del desarrollo tecnológico, que, a pesar de ser necesarias, requieren mayor madurez regulatoria, lo que las ubica como estrategias que van de mediano a largo plazo. Asimismo, la implementación de herramientas tecnológicas de supervisión y la inversión en ciberseguridad, si bien son relevantes, dependen de condiciones habilitantes como capacidades técnicas, presupuesto y gobernanza digital efectiva.

Este análisis permite establecer una hoja de ruta estratégica, que prioriza intervenciones de alto retorno institucional y social, con una visión de escalabilidad progresiva que permita construir, desde la base, una gobernanza digital sólida, adaptativa, centrada en la privacidad y en la protección efectiva de los derechos de las personas.

### 6.3. IDENTIFICACIÓN DE EJES ESTRATÉGICOS



*Ilustración 2 Imagen creada por inteligencia artificial por los autores PNPD*

Los tres ejes estratégicos propuestos en este Plan, abordan de manera integral los principales desafíos en materia de protección de datos personales en el Ecuador. El fortalecimiento de la gobernanza digital busca consolidar una estructura institucional sólida.

Por su parte, la universalización del derecho a la protección de datos y la promoción de la cultura ciudadana apunta a cerrar brechas de conocimiento, acceso y ejercicio efectivo de este derecho, mediante la formación y sensibilización de la población sobre el uso ético y responsable de la información personal.

Finalmente, el eje de innovación y vigilancia digital para un ecosistema nacional seguro se orienta hacia el uso de tecnologías emergentes y al fortalecimiento de capacidades técnicas que permitan prevenir riesgos, detectar vulnerabilidades y responder de manera efectiva ante incidentes que comprometan la seguridad y privacidad de los datos.

#### OBJETIVO ESTRATÉGICO 1: Fortalecimiento de la gobernanza institucional

*“Consolidar una estructura institucional integral, robusta, coordinada y eficaz que incluya a sus actores y que viabilice garantías efectivas para la protección de datos personales, la transparencia, la rendición de cuentas y el respeto al derecho mediante el cumplimiento normativo en todos los niveles de la administración pública y privada”.*



*Ilustración 3 Imagen creada por inteligencia artificial por los autores - Objetivo Estratégico #1*

La digitalización de los servicios públicos y privados, así como el creciente uso intensivo de datos personales en procesos administrativos, operativos y tecnológicos, ha generado desafíos para garantizar la protección efectiva de la información personal de los ciudadanos. En este contexto, la gobernanza en protección de datos se convierte en un pilar fundamental para consolidar instituciones a la vanguardia, responsables y transparentes.

Este eje estratégico propone el fortalecimiento integral de la gobernanza institucional en materia de protección de datos personales, a través del diseño, generación y aplicación de marcos normativos, la definición de roles y responsabilidades, la conformación de estructuras funcionales (como comités, responsables y unidades técnicas especializadas) y el desarrollo de capacidades

permanentes.

Asimismo, promueve la articulación entre los diferentes actores institucionales y sectores, para impulsar espacios de coordinación y cooperación, mecanismos de monitoreo y evaluación continua que aseguren el cumplimiento normativo y la mejora continua de los procesos. Se busca fomentar una cultura organizacional basada en la privacidad como derecho fundamental.

Este enfoque de gobernanza reconoce que la protección de datos no es solo una obligación legal, sino una condición indispensable para fortalecer la confianza pública, la legitimidad institucional y la integridad de los servicios ofrecidos en el entorno digital.



**ESTRATEGIA 1:** Diseñar y consolidar marcos normativos y procedimentales internos a fin de garantizar que cada entidad cuente con reglas claras, actualizadas y vinculantes sobre el debido tratamiento de datos personales.

**Acciones relevantes:**

- Elaboración de reglamentos internos, estándares o manuales de protección de datos que permitan la implementación de PDP en todas sus categorías.
- Integración de cláusulas de protección de contratos, convenios y procesos administrativos, así como también la definición de roles y responsabilidades.
- Revisión y actualización periódica de políticas de privacidad y procedimientos, así como el establecimiento de protocolos para la atención oportuna de los derechos establecidos en la LOPDP.
- Adopción de medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos detectados y las potenciales vulneraciones que pudieren sobrevenir sobre datos personales.

**ESTRATEGIA 2:** Fortalecer las capacidades técnicas y operativas que permitan asegurar que los funcionarios cuenten con los conocimientos y herramientas necesarios para aplicar adecuadamente la normativa.

**Acciones relevantes:**

- Diseño e implementación de programas de formación continua, así como fortalecimiento de los equipos técnicos responsables mediante dotación de recursos tecnológicos y humanos.
- Desarrollo de guías y recursos prácticos adaptados a los diferentes niveles institucionales y certificación de funcionarios responsables en buenas prácticas de protección de datos.
- Inclusión de módulos sobre protección de datos en planes de inducción institucional.

**ESTRATEGIA 3:** Establecer mecanismos de coordinación y articulación interinstitucional a fin de lograr coherencia y colaboración entre entidades públicas, privadas y de la sociedad civil.

**Acciones relevantes:**

- Creación de comités y redes interinstitucionales de protección de datos, y establecimiento de canales formales de comunicación entre organismos.
- Promoción de convenios de colaboración para intercambio de buenas prácticas y herramientas, así como participación en espacios regionales e internacionales sobre protección de datos.
- Desarrollo de estrategias comunes de respuesta ante incidentes de seguridad de la información.

**Tabla 2** Metas e indicadores – OE1

| META                                                                                                                                                                                               | INDICADOR                                                                                                                                                                     | PLAZO     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 80 % de los responsables del tratamiento de datos en instituciones públicas y privadas priorizadas serán capacitados en normativa de protección de datos personales.                               | Porcentaje de responsables del tratamiento de datos personales del sector público y privado capacitados y certificados en buenas prácticas de protección de datos personales. | 2025-2027 |
| 80% de las entidades públicas priorizadas contarán con normas y procedimientos internos actualizados, vinculantes y en funcionamiento, que garanticen el tratamiento adecuado de datos personales. | Porcentaje de entidades públicas que implementan efectivamente la normativa y los procedimientos internos para la protección de datos personales.                             | 2026-2028 |
| Creación e implementación del sistema para el Registro Nacional de Protección                                                                                                                      | Porcentaje de entidades que participan en el sistema del Registro                                                                                                             | 2025-2029 |



| META                                                                                                                                                                                         | INDICADOR                                   | PLAZO |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-------|
| de Datos Personales, con al menos el 70% de participación de entidades del sector público que cuenten con protocolos conjuntos para la gestión de incidentes de seguridad de la información. | Nacional de Protección de Datos Personales. |       |

**Elaboración:** Superintendencia de Protección de Datos Personales.

**Actores directos:** Ministerio de Telecomunicaciones y de la Sociedad de la Información, Ministerio de Inclusión Económica y Social, Ministerio de Economía y Finanzas, Ministerio de Salud Pública, Ministerio de Educación, Instituto Nacional de Estadística y Censos, Defensoría del Pueblo, Consejo Nacional para la Igualdad de Discapacidades y Función de Transparencia de Control Social.

## **OBJETIVO ESTRATÉGICO 2: Universalización del derecho a la protección de datos y promoción de la cultura ciudadana**

*“Desarrollar una cultura ciudadana, a fin de que se fomente el uso responsable y ético de la información personal, especialmente en entornos digitales, con el fin de cerrar las brechas territoriales, tecnológicas y culturales mediante el conocimiento, acceso y ejercicio de manera efectiva de los derechos establecidos en la LOPDP”.*



**Ilustración 4** Imagen creada por inteligencia artificial por los autores - Objetivo Estratégico #2

Garantizar que todas las personas en el territorio ecuatoriano, sin importar su ubicación geográfica, condición social, nivel educativo o lenguaje nativo, conozcan, accedan y ejerzan de manera efectiva los derechos establecidos en la LOPDP, de tal manera que se promueva una cultura ciudadana digital que fomente el uso responsable, ético e informado de la información personal, especialmente en entornos tecnológicos.

La protección de datos personales debe ser entendida como un derecho fundamental que trasciende las fronteras individuales y se universaliza en la sociedad digital contemporánea. La universalización de los derechos de protección de datos personales busca asegurar que cada individuo tenga control sobre su información personal, para así garantizar su dignidad y privacidad<sup>11</sup>.

La promoción de una cultura ciudadana en relación con la protección de datos es esencial para empoderar a las personas. Esto implica capacitar y sensibilizar a la población sobre sus derechos en el manejo de datos personales y la importancia de la privacidad en un mundo interconectado. Al fomentar esta conciencia, se promueve un entorno donde los ciudadanos pueden ejercer plenamente sus derechos y participar activamente en la sociedad de manera segura.

En este sentido, la acción coordinada entre el Estado con las diferentes instituciones públicas, las comunidades y los demás actores sociales, busca cerrar las brechas territoriales, tecnológicas y culturales en el ejercicio del derecho fundamental a la protección de datos personales.

**ESTRATEGIA 1:** Desarrollar e implementar programas de capacitación dirigidos a diversas poblaciones, que incluya talleres, charlas y recursos digitales que aborden la importancia de la

<sup>11</sup> Rawls, J. (1999). *A Theory of Justice*. Harvard University Press.



protección de datos personales y los derechos asociados; programas que deberán ser capaces de adaptarse a diferentes contextos culturales, niveles educativos y lenguas nativas.

### Acciones relevantes:

- Colaborar con unidades educativas, universidades y organizaciones comunitarias para facilitar el acceso a la formación en materia de protección de datos personales.
- Crear materiales didácticos accesibles y culturalmente relevantes, comprensibles para todos los estratos de la población y en sus lenguas nativas.

**ESTRATEGIA 2:** Crear plataformas digitales que ofrezcan información clara y accesible sobre el derecho de protección de datos, así como herramientas para que los ciudadanos puedan gestionar su información personal de manera segura. Estas plataformas deberán ser inclusivas y accesibles, considerando la diversidad lingüística, las condiciones socioeconómicas de los usuarios y su pertenencia a grupos de atención prioritaria.

### Acciones relevantes:

- Diseñar una interfaz amigable para los ciudadanos, sin exclusiones del nivel de alfabetización digital.
- Ofrecer soporte en múltiples lenguas nativas y de señas, contenidos multimedia, así como formatos descargables y de impresión.
- Garantizar la accesibilidad de recursos educativos para personas con discapacidad y neurodiversas, por medio de estándares de accesibilidad web, fuentes ajustables y navegación simplificada.

**ESTRATEGIA 3:** Establecer un marco de cooperación entre el Estado, instituciones públicas, ONGs y actores sociales para implementar iniciativas que cierren las brechas territoriales y tecnológicas en el ejercicio del derecho a la protección de datos, incluida la creación de redes de apoyo y la promoción de políticas públicas inclusivas.

### Acciones relevantes:

- Organizar mesas de trabajo con representantes de diferentes sectores.
- Realizar diagnósticos en territorio sobre el ejercicio del derecho a la protección de datos.
- Implementar proyectos piloto en áreas vulnerables a fin de generar redes locales de alfabetización en protección digital.

**Tabla 3** Metas e indicadores – OE2

| META                                                                                                                                                                                    | INDICADOR                                                                                      | PLAZO     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-----------|
| El 20% de las unidades educativas habrá recibido formación accesible y culturalmente adaptada sobre protección de datos personales.                                                     | Porcentaje de unidades educativas capacitadas                                                  | 2025-2029 |
| Contar con al menos 1 plataforma digital inclusiva, intercultural y accesible, que permita a los ciudadanos informarse, cumpliendo con estándares internacionales de accesibilidad web. | Porcentaje de usuarios que han accedido y utilizado las plataformas digitales para informarse. | 2025-2029 |
| Fomentar 8 mesas de trabajo técnicas con representantes de diferentes sectores para el fortalecimiento de protección de datos personales en territorio.                                 | Número de mesas de trabajo en territorio.                                                      | 2025-2029 |

**Elaboración:** Superintendencia de Protección de Datos Personales.



**Actores directos:** Ministerio de Telecomunicaciones y de la Sociedad de la Información, Ministerio de Inclusión Económica y Social, Ministerio de Economía y Finanzas, Ministerio de Salud Pública, Ministerio de Educación, Defensoría del Pueblo y Academia.

### **OBJETIVO ESTRATEGICO 3: Innovación digital para un ecosistema seguro**

*“Fortalecer el ecosistema nacional de protección de datos mediante la adopción de tecnologías emergentes para prevenir y mitigar riesgos en el tratamiento de información personal”.*



*Ilustración 5 Imagen creada por inteligencia artificial por los autores - Objetivo Estratégico #3*

Este eje estratégico impulsa la transformación digital responsable del Ecuador, mediante la integración de tecnologías emergentes (como inteligencia artificial, blockchain, big data, análisis predictivo y automatización de auditorías) a la implementación de la protección de datos personales en el país. Esta integración debe tener como finalidad el mejoramiento de la productividad en las estrategias, operaciones y tácticas utilizadas para la administración pública, desde un enfoque de gestión de riesgos multidimensional.

En este contexto, es necesario desarrollar métricas y modelos adecuados de riesgo a fin de incrementar la productividad desde el diseño y por defecto y, a la vez, proteger los derechos y libertades de las personas naturales. Su objetivo es fortalecer la capacidad de las instituciones y del Estado para prevenir, detectar y mitigar riesgos tecnológicos, que asegure una gobernanza digital sólida, proactiva y adaptativa frente a nuevas amenazas. Consecuentemente, es necesario fomentar una política pública fundamentada en la gestión de riesgos que permita disminuir la incertidumbre en los procesos que involucran a las personas naturales, con el fin de tomar decisiones informadas.

Además, este eje promueve la incorporación del principio de privacidad por diseño en los sistemas públicos y privados, para asegurar que el tratamiento de datos personales esté alineado desde su origen con los más altos estándares de seguridad, ética digital y cumplimiento normativo.

**ESTRATEGIA 1:** Desarrollar e implementar el Registro Nacional de Protección de Datos, que permita a las entidades públicas y privadas cumplir con las previsiones del artículo 51 de la LOPDP.

#### **Acciones relevantes:**

- Implementar sistemas de análisis de datos sobre cumplimiento normativo, que utilice inteligencia artificial para la detección de alertas y brechas en los procesos de control y sanción.
- Fomentar el trabajo conjunto entre la SPDP y los sujetos regulados para el desarrollo e implementación del Registro Nacional de Protección de Datos, lo que facilitará la integración de las entidades públicas y privadas en la gestión y cumplimiento normativo.
- Facilitar la identificación de las actividades del tratamiento de datos personales de los sujetos regulados.

**ESTRATEGIA 2:** Promover una mejor toma de decisiones fundamentada en la gestión de riesgos para la protección de derechos y libertades de los titulares de datos.



**Acciones relevantes:**

- Desarrollar guías que promuevan principios de gestión de riesgos fundamentados en la objetividad, eficacia, y eficiencia.
- Promover la identificación constante de vulnerabilidades de sistemas de información que puedan afectar los derechos de las personas.
- Incentivar proyectos ciudadanos para mejorar la práctica regulatoria en temas vinculados a tecnologías emergentes.

**ESTRATEGIA 3:** Impulsar alianzas estratégicas con universidades, centros de investigación y empresas tecnológicas para la protección de datos personales.

**Acciones relevantes**

- Firmar convenios de cooperación interinstitucional para la investigación aplicada en tecnologías de protección de datos.
- Crear convocatorias nacionales de innovación abierta para financiar soluciones tecnológicas para la protección de datos personales.
- Promover la participación de estudiantes, investigadores y desarrolladores ecuatorianos en proyectos piloto vinculados a la privacidad y ciberseguridad de datos personales.

**Tabla 4** Metas e indicadores – OE3

| META                                                                                                                                                                                                                | INDICADOR                                                                                                                                                                       | PLAZO     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Registro Nacional de Protección de Datos integrará con al menos el 70% de las instituciones públicas y empresas privadas.                                                                                           | Porcentaje de las instituciones públicas y empresas privadas integradas activamente en el Registro Nacional de Protección de Datos.                                             | 2025-2026 |
| El 70% de las infraestructuras digitales de los sectores de salud pública, educación, justicia, seguridad y servicios sociales estarán ajustadas a la metodología de gestión de riesgos para la toma de decisiones. | Porcentaje de instituciones públicas y empresas privadas que implementen métodos de gestión de riesgos fundamentados en métricas significativas y modelos adecuados de riesgos. | 2025-2028 |
| Contar con un ecosistema nacional activo de investigación e innovación en tecnologías emergentes aplicadas a la protección de datos personales, con al menos 5 instituciones académicas.                            | Número de instituciones académicas, centros de investigación y empresas tecnológicas que participan activamente en proyectos de innovación en protección de datos personales.   | 2025-2028 |

**Elaboración:** Superintendencia de Protección de Datos Personales.

**Actores directos:** Ministerio de Telecomunicaciones y de la Sociedad de la Información, Ministerio de Inclusión Económica y Social, Ministerio de Economía y Finanzas, Ministerio de Salud Pública, Ministerio de Educación, Defensoría del Pueblo, Consejo Nacional para la Igualdad de Discapacidades, Corte Constitucional y Función de Transparencia de Control Social.



#### 6.4. Proyectos y Presupuesto Referencial

### “PROGRAMA INTEGRAL DE PROTECCIÓN DE DATOS PERSONALES Y CONFIANZA DIGITAL”

**Tabla 5** Presupuesto referencial por año

| Proyectos                                              | Unidad responsable | Año 1                   | Año 2           | Año 3           | Año 4           | Total           |
|--------------------------------------------------------|--------------------|-------------------------|-----------------|-----------------|-----------------|-----------------|
| Fortalecimiento de la gobernanza                       | IRD                | \$ 626.474,40           | \$ 2.103.997,31 | \$ 1.596.570,53 | \$ 1.583.333,33 | \$ 5.910.375,58 |
| Universalización del derecho y promoción de la cultura | IRD                | \$ 924.475,00           | \$ 1.442.332,14 | \$ 1.632.808,33 | \$ 2.966.141,67 | \$ 6.965.757,14 |
| Innovación digital para un ecosistema seguro           | IIT                | \$ 678.333,33           | \$ 1.346.190,48 | \$ 1.536.666,67 | \$ -            | \$ 3.561.190,48 |
| <b>TOTAL</b>                                           |                    | <b>\$ 16.437.475,20</b> |                 |                 |                 |                 |

**Elaboración:** Superintendencia de Protección de Datos Personales.

### 7. VINCULACIÓN DEL PLAN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES CON AGENDA ODS 2030 Y EL PLAN NACIONAL DE DESARROLLO.

#### 7.1. Agenda Objetivos de Desarrollo Sostenible 2030:

A continuación se muestra cómo las acciones y estrategias orientadas a garantizar el tratamiento ético, seguro y transparente de los datos personales se articulan directamente con diversos Objetivos de Desarrollo Sostenible.

**Tabla 6** Alineación del PNPDP con la Agenda 2030

| ODS                                              | Meta relacionada                                                                                  | Vinculación con la PDP                                                                                                                      |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>3</b> Salud y bienestar                       | (No específica, relevante en salud digital)                                                       | El uso ético de datos de salud protege la privacidad de los pacientes y garantiza la confianza en los sistemas sanitarios digitales.        |
| <b>4</b> Educación de calidad                    | 4.4 – Habilidades para el empleo y tecnologías.<br>4.7 – Educación para la ciudadanía global.     | La alfabetización digital abarca el conocimiento de los derechos en el entorno digital e incluye la privacidad y el uso ético de los datos. |
| <b>8</b> Trabajo decente y crecimiento económico | 8.5 – Empleo pleno y productivo, y trabajo decente                                                | En el medio laboral digital, la protección de datos previene el abuso y garantiza un trato justo en el uso de información personal.         |
| <b>9</b> Industria, innovación e infraestructura | 9.c – Aumentar el acceso a tecnologías de la información y comunicación, y tecnologías digitales. | Asegura el desarrollo de infraestructuras digitales seguras y respetuosas con la privacidad, y fomenta una innovación responsable.          |
| <b>10</b> Reducción de desigualdades             | 10.2 – Promover inclusión social, económica y política.                                           | La protección de datos previene la discriminación y el uso indebido de información de grupos vulnerables, lo que promueve la equidad.       |
| <b>16</b> Paz, justicia e instituciones sólidas  | 16.10 – Garantizar el acceso público a la información y proteger libertades fundamentales.        | Al ser la protección de datos personales un derecho fundamental, refuerza el estado de derecho, la transparencia y la confianza ciudadana.  |

**Elaboración:** Superintendencia de Protección de Datos Personales.



## 7.2. Articulación con el Plan Nacional de Desarrollo 2024 - 2025

A continuación, se muestra la alineación de los ejes estratégicos del Plan Nacional de Protección de Datos Personales propuestos por la Superintendencia, con el Plan Nacional de Desarrollo 2024 – 2025:

**Tabla 7** Articulación de los Objetivos del Plan PDP con objetivos y políticas del PND

| Objetivo del PND                                                                                                            | Políticas                                                                                                                                                            | Objetivos del PNPDP |
|-----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| 3. Garantizar la seguridad integral, la paz ciudadana y transformar el sistema de justicia respetando los derechos humanos. | 3.12. Contribuir al fortalecimiento de la ciberseguridad en el sector de las telecomunicaciones.                                                                     | 3                   |
| 9. Propender la construcción de un Estado eficiente, transparente y orientado al bienestar social.                          | 9.3 Fomentar buenas prácticas regulatorias y la simplificación normativa y administrativa que promueva la innovación de la gestión pública.                          | 1                   |
|                                                                                                                             | 9.7 Ampliar y fortalecer la cooperación internacional para el desarrollo sostenible del Ecuador en función de las prioridades determinadas por el Gobierno Nacional. | 2                   |

**Elaboración:** Superintendencia de Protección de Datos Personales.

Como se puede evidenciar en la tabla anterior, el Plan Nacional de Desarrollo vigente **no contiene una política específica en relación con el derecho a la protección de datos personales** en el Ecuador, lo que genera la necesidad de contar con mecanismos desde la planificación nacional, a fin de garantizar el derecho fundamental a la privacidad de los datos en el país.

## 8. CONCLUSIONES Y RECOMENDACIONES

El Plan Nacional de Protección de Datos Personales demuestra que la privacidad y protección de los datos en la sociedad ecuatoriana requiere una sólida estructura institucional, cultural y normativa, que garantice el derecho a la protección de los datos.

Si bien el país ha mostrado avances importantes tras la promulgación de la LOPDP, su Reglamento General y la puesta en marcha de la SPDP, persisten desafíos estructurales que limitan su aplicación efectiva e impacto real en los ciudadanos. Por ello, se impulsa el reconocimiento de la protección de datos personales como una política pública prioritaria transversal. Consecuentemente, se han analizado diversas estrategias y acciones que permitan el fortalecimiento institucional, la implementación de la normativa y la capacitación técnica, considerándolas como claves para avanzar hacia una gobernanza sólida y proactiva en protección de datos.

A través de sus ejes estratégicos (el fortalecimiento de la gobernanza digital, la universalización del derecho a la protección de datos, la promoción de una cultura ciudadana, así como la innovación digital para un ecosistema seguro), se propone dar una solución planificada, realista, escalonada y, a la vez, integral para la debida protección de los datos personales. Esta hoja de ruta permitirá consolidar un entorno digital ético, seguro y respetuoso de este derecho fundamental en el Ecuador.

Ante este panorama, se recomienda consolidar una gobernanza nacional en materia de protección de datos personales que articule todos los niveles del Estado y que promueva la corresponsabilidad entre actores públicos, privados y sociales, para garantizar la efectiva vigencia y el cabal cumplimiento del marco legal vigente y complementario.



## **9. GLOSARIO**

**CRE:** Constitución de la República del Ecuador.

**IA:** Inteligencia Artificial.

**LOPDP:** Ley Orgánica de Protección de Datos Personales.

**OCDE:** Organización para la Cooperación y el Desarrollo Económico.

**ODS:** Objetivos de Desarrollo Sostenible.

**OEА:** Organización de Estados Americanos.

**ONG:** Organismo No Gubernamental

**ONU:** Organización de las Naciones Unidas.

**PDP:** Protección de Datos Personales.

**PND:** Plan Nacional de Desarrollo.

**PNPDP:** Plan Nacional de Protección de Datos Personales.

**RGPD:** Reglamento General de Protección de Datos.

**SPDP:** Superintendencia de Protección de Datos Personales.

**TICs:** Tecnologías de la Información y Comunicación.

**UE:** Unión Europea.



## **10. REFERENCIAS**

- Constitución de la República del Ecuador. (2008, 20 de octubre). Registro Oficial, No. 449. Modificado el 20 de enero de 2021. <https://www.asambleanacional.gob.ec/es/leyes-y-constitucion>
- Consejo de Europa. (1981, 28 de enero). Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108). <https://www.coe.int/en/web/data-protection/convention108>
- Unión Europea. (2016, 27 de abril). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo: Reglamento General de Protección de Datos (RGPD). Diario Oficial de la Unión Europea. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2013). Recomendación del Consejo sobre los principios de privacidad y flujo transfronterizo de datos personales. <https://www.oecd.org/sti/ieconomy/oecd-privacy-framework.pdf>
- Organización de las Naciones Unidas (ONU). (2013, 18 de diciembre). Resolución 68/167 sobre el derecho a la privacidad en la era digital. <https://undocs.org/es/A/RES/68/167>
- Organización de los Estados Americanos (OEA). (2001, 11 de septiembre). Carta Democrática Interamericana. <https://www.oas.org/es/democratica/carta.asp>
- Regnier, P. (1979). L'Abacus: Une méthode d'évaluation intuitive des projets. Bruxelles: Université Libre de Bruxelles.
- Fundación Ciudadanía y Desarrollo. (2024, septiembre). Informe de entrevista a expertos: Guía de Protección de Datos Personales - Ecuador.



## **11. ANEXOS**

1. Cronograma para el levantamiento de Políticas Públicas en materia de Protección de Datos Personales.
2. Memorando N° SPDP-SPD-2025-0028-M Quito, D. M., marzo 12 del 2025, Asignación del equipo técnico multidisciplinario para el levantamiento de políticas públicas.
3. Memorando N° SPDP-PGE-2025-0056-M Quito, D. M., marzo 12 del 2025, Solicitud de aprobación de instrumentos para el diagnóstico de Políticas Públicas en materia de protección de datos personales.
4. Encuesta de percepción ciudadana sobre protección de datos personales.
5. Entrevista a expertos en protección de datos personales.
6. Informe de análisis de resultados de las encuestas a la ciudadanía y entrevistas a expertos.