

**CONSEJO DIRECTIVO
NOVENA SESION ORDINARIA
Lima, 21 de Junio de 2022**

ACUERDO N° 17-9-ESSALUD-2022

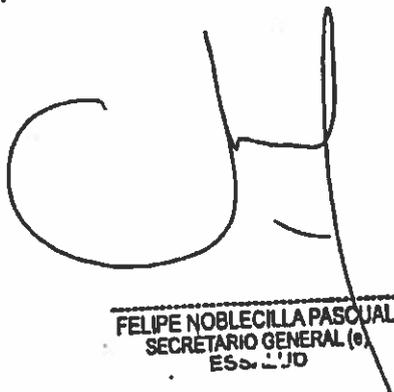
VISTOS:

Los Memorandos Nros. 609 y 832-GCTIC-ESSALUD-2022, de la Gerencia Central de Tecnologías de Información y Comunicaciones, con los que se propone la aprobación de la *"Política Institucional de Protección de Datos Personales"*; el Memorando N° 4038-GCPP-ESSALUD-2022 e Informe N° 118-GOP-GCPP-ESSALUD-2022 de la Gerencia Central de Planeamiento y Presupuesto; el Memorando N° 2172-GCAJ-ESSALUD-2022 e Informe N° 250-GNA-GCAJ-ESSALUD-2022 de la Gerencia Central de Asesoría Jurídica; y el Memorando N° 1378-GG-ESSALUD-2022 de la Gerencia General, y;

En virtud de las facultades conferidas, por mayoría, el Consejo Directivo;

ACORDÓ:

1. APROBAR la *"Política Institucional de Protección de Datos Personales"*.
2. DISPONER que la Gerencia Central de Tecnologías de Información y Comunicaciones emita las disposiciones y/o realice las acciones necesarias, para la implementación de la política aprobada en el numeral 1 del presente Acuerdo.
3. EXONERAR el presente Acuerdo del trámite de lectura y aprobación del acta para su inmediata ejecución.


FELIPE NOBLECILLA PASCUAL
SECRETARIO GENERAL (e)
ESSALUD



POLÍTICA INSTITUCIONAL DE PROTECCIÓN DE DATOS PERSONALES



Versión	Fecha	Elaborado:	Revisado:	Aprobado:
V1.0		Gerencia Central de Tecnologías de Información y Comunicaciones	Gerencia Central de Planeamiento y Presupuesto. Gerencia Central de Asesoría Jurídica.	Consejo Directivo



**POLÍTICA INSTITUCIONAL DE PROTECCIÓN
DE DATOS PERSONALES**

P-PDP/001-OSI-GCTIC
90-2022
V1.0

CONTENIDO

1.	Introducción.....	3
2.	Objetivo.....	3
3.	Marco Normativo.....	3
4.	Ámbito de Aplicación.....	4
5.	Lineamientos para la protección de datos personales.....	4
6.	Definiciones.....	6
7.	Declaración de la Política Institucional de Protección de Datos Personales.....	9





POLÍTICA INSTITUCIONAL DE PROTECCIÓN DE DATOS PERSONALES

P-PDP/001-OSI-GCTIC
90-2022
V1.0

1. Introducción

La Ley de Protección de Datos Personales N° 29733, tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen. Mediante el Decreto Supremo N° 003-2013-JUS del 08 de mayo del 2013, regulando un adecuado tratamiento, tanto por las entidades públicas, como por las instituciones pertenecientes al sector privado. Sus disposiciones constituyen normas de orden público y de cumplimiento obligatorio.

El Seguro Social de Salud – ESSALUD, consciente de la responsabilidad que le asiste en materia de Tratamiento de Datos Personales, garantiza el derecho constitucional que tienen todas las personas a conocer, actualizar, rectificar, suprimir y revocar el consentimiento respecto a los datos personales que hayan recogido sobre ellas en los bancos de datos personales de la Entidad, las cuales han sido tratadas conforme a lo establecido por la Ley de Protección de Datos Personales y su Reglamento.

Para tales efectos el Seguro Social de Salud –ESSALUD, ha elaborado la presente POLÍTICA INSTITUCIONAL DE PROTECCIÓN DE DATOS PERSONALES, cuya aplicación es de carácter obligatorio para todas las personas naturales o jurídicas que hagan tratamiento de los datos personales registrados en los Bancos de Datos de la Entidad, con el fin de proporcionar los lineamientos necesarios para el cumplimiento de las obligaciones legales en materia de protección de datos personales.

2. Objetivo

Establecer el marco general para la gestión adecuada del tratamiento de datos personales en el Seguro Social de Salud – ESSALUD, asegurando el respeto del derecho al honor y a la intimidad en el tratamiento de las diferentes tipologías de datos personales, procedentes de diferentes fuentes y con fines diversos en función a actividades de otorgamiento de prestaciones de prevención, promoción, recuperación, rehabilitación, prestaciones económicas, y prestaciones sociales, en el marco de las funciones asignadas a ESSALUD.

3. Marco Normativo

- 3.1. Ley N° 27056, Ley de Creación del Seguro Social de Salud - ESSALUD y su Reglamento, aprobado por Decreto Supremo N° 002-99-TR, y sus modificatorias.
- 3.2. Ley N° 30096, Ley de delitos informáticos, y sus modificatorias.
- 3.3. Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento, aprobado por Decreto Supremo N° 003-2013-JUS, y sus modificatorias.
- 3.4. Decreto Supremo N° 021-2019-JUS Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública
- 3.5. Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.
- 3.6. Decreto Supremo N° 072-2013-PCM, que aprueba el Reglamento de la Ley de Transparencia y Acceso a la Información Pública, y sus modificatorias
- 3.7. Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo



	POLÍTICA INSTITUCIONAL DE PROTECCIÓN DE DATOS PERSONALES	P-PDP/001-OSI-GCTIC 90-2022 V1.0
---	---	---

- 3.8. Decreto Legislativo N° 1353, Decreto Legislativo que crea la autoridad Nacional de Transparencia y Acceso a la Información Pública. Fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses.
- 3.9. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
- 3.10. Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición, en todas las Entidades integrantes del Sistema Nacional de Informática.
- 3.11. Resolución Ministerial N° 688-2020/MINSA, que aprueba la Directiva Administrativa N° 294-MINSA/2020/OGTI, Directiva Administrativa que establece el tratamiento de los datos personales relacionados con la salud o datos personales en salud.
- 3.12. Resolución de Presidencia Ejecutiva N° 767-PE-ESSALUD-2015, que aprueba el Texto Actualizado y Concordado del Reglamento de Organización y Funciones del Seguro Social de Salud - ESSALUD, y sus modificatorias.

4. Ámbito de Aplicación

La Política Institucional de Protección de Datos Personales, involucra a todas las unidades de organización del Seguro Social de Salud. Es dirigida al personal indistintamente de su régimen laboral, modalidad de contratación y nivel jerárquico; así como a las personas naturales o jurídicas que prestan servicios a la institución, con quienes se hayan suscrito contratos o convenios y tengan acceso a datos personales y a la red de datos de la entidad a nivel nacional.

5. Principios para la protección de datos personales

Los siguientes principios guían el adecuado tratamiento de los datos personales:

- 5.1. **Legalidad:** El tratamiento de datos personales realizado por ESSALUD se hará conforme a lo dispuesto en la Ley de Protección de Datos Personales. Se encuentra prohibida la recopilación de datos personales por medios fraudulentos, desleales o ilícitos.¹
- 5.2. **Consentimiento:** ESSALUD no podrá tratar datos personales que no cuenten con el consentimiento informado, previo, expreso, inequívoco y libre de su titular según sea necesario, salvo las excepciones previstas por Ley. Los órganos que registren datos personales deberán adoptar procedimientos y/o elaborar formatos para el cumplimiento de esta disposición².
- 5.3. **Limitaciones al consentimiento para el tratamiento de datos personales:** No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:
 - 5.3.1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.³
 - 5.3.2. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.⁴



¹ Ley de Protección de Datos Personales, Artículo 4, Principio de legalidad.

² Ley de Protección de Datos Personales, Artículo 5, Principio de consentimiento.

³ Ley N° 29733, Artículo 14, numeral 1.

⁴ Ley N° 29733, Artículo 14, numeral 2.

- 5.3.3. Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.⁵
- 5.3.4. Cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.⁶
- 5.3.5. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.⁷
- 5.3.6. Cuando se hubiera aplicado un procedimiento de anonimización o disociación.⁸
- 5.3.7. Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de tratamiento de datos personales.⁹
- 5.3.8. Cuando el tratamiento sea para fines vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo u otros que respondan a un mandato legal.¹⁰
- 5.4. **Finalidad:** Los datos personales objeto de tratamiento no podrán ser utilizados para fines distintos o incompatibles con aquellos que motivaron su obtención, salvo consentimiento de su titular.¹¹
- 5.5. **Proporcionalidad:** Todo tratamiento de datos personales realizado por ESSALUD deberá ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.¹²
- 5.6. **Calidad:** Los datos personales que vayan a ser tratados por ESSALUD deben ser veraces, exactos y, en la medida de lo posible, actualizada, necesaria, pertinente y adecuada respecto de la finalidad para la que fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir



5 Ley N° 29733, Artículo 14, numeral 4.

6 Ley N° 29733, Artículo 14, numeral 5.

7 Ley N° 29733, Artículo 14, numeral 6.

8 Ley N° 29733, Artículo 14, numeral 8.

9 Ley N° 29733 Ley de Protección de Datos Personales, Artículo 14, numeral 9.

10 Ley N° 29733 Ley de Protección de Datos Personales, Artículo 14, numeral 10.

11 Ley N° 29733 Ley de Protección de Datos Personales, Artículo 6, Principio de finalidad.

12 Ley N° 29733 Ley de Protección de Datos Personales, Artículo 7, Principio de proporcionalidad.

con la finalidad del tratamiento respetando los plazos legales de conservación de documentos e información aplicables. Las correcciones de datos personales en los que sea necesaria la intervención de la Gerencia Central de Tecnologías de Información Comunicaciones deben realizarse siempre a solicitud del propietario de la información.¹³

5.7. Principio de seguridad: El titular del banco de datos personales y el encargado o responsable del tratamiento de los Bancos de Datos Personales deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.¹⁴

5.7.1. Seguridad de la Información: La entidad debe estar conforme a la norma ISO 27001 que abarcan políticas en la seguridad de la información, el acceso a la información, los sistemas, la informática en la nube, la seguridad de las aplicaciones, la clasificación de la información y las normas de seguridad vigentes.¹⁵

5.8. Principio de disposición de recurso: ESSALUD debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.¹⁶

5.9. Principio de nivel de protección adecuado: Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por la Ley o por los estándares internacionales en la materia.¹⁷

6. Definiciones

6.1. Activo de Información:

Cualquier dato, información o elemento que tiene valor para la Entidad (software, equipos de cómputo y telecomunicaciones, servicio de correo electrónico, servicio de internet, archivadores, formularios, historias clínicas, entre otros) y que por lo tanto requiere protección.¹⁸

6.2. Banco de datos personales:

Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.¹⁹

6.3. Banco de datos personales no automatizado:

Conjunto de datos de personas naturales no computarizado y estructurado conforme a criterios específicos, que permita acceder sin esfuerzos desproporcionados a los datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.²⁰



¹³ Ley N° 29733 Ley de Protección de Datos Personales, Artículo 8. Principio de calidad.

¹⁴ Ley N° 29733 Ley de Protección de Datos Personales, Artículo 9. Principio de seguridad.

¹⁵ OMS/ Políticas/Políticas de publicación/Política de datos

¹⁶ Ley N° 29733 Ley de Protección de Datos Personales, Artículo 10. Principio de disposición de recurso.

¹⁷ Ley N° 29733 Ley de Protección de Datos Personales, Artículo 11. Principio de nivel de protección adecuado.

¹⁸ Adaptado del Numeral 8.2.2 Identificación de activos, NTP-ISO/IEC 27005:2018

¹⁹ Ley de Protección de Datos Personales, Artículo 2. Numeral 1, Definiciones

²⁰ Reglamento de la Ley N° 29733 Ley de Protección de Datos Personales, Artículo 2. Definiciones, Numeral 1.

6.4. Confidencialidad de la Información:

Es un atributo que se le asigna a la información por la naturaleza de su contenido o por los principios que rigen a quien accede a esa información, eso hace que el contenido solo pueda ser accedido por personas autorizadas o tomen conocimiento en ejercicio de su labor, quienes tienen el deber de reservar dicha información y no comentar o divulgar la misma fuera del ámbito estrictamente profesional o para la prestación de servicios. La organización o Entidad garantiza que la información será protegida para que sea conocida solo por usuarios autorizados.²¹

6.5. Consentimiento para el Tratamiento de Datos Personales:

Es un principio establecido en la Ley N° 29733, Ley de Protección de Datos Personales, el cual permite que el tratamiento de los datos personales sea lícito cuando el titular del dato personal hubiere prestado su consentimiento libre, previo, expreso, informado e inequívoco.²²

6.6. Derecho de Información del titular de datos personales:

Es el Derecho que tiene el titular de datos personales, en vía de acceso, a que se le brinde toda la información señalada sobre: La finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del o del responsable o encargados del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello. Así también, toda la información señalada en el artículo 18 de la Ley de protección de datos personales y el numeral 4 del artículo 12 de su reglamento²³.

6.7. Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición):

Es el conjunto de derechos a través de los cuales la Ley N° 29733 – Ley de Protección de Datos Personales, garantiza a las personas el poder de control sobre sus datos personales.²⁴

6.8. Datos personales:

Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.²⁵

6.9. Datos sensibles:

Son los datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual. Filiación sindical; e información relacionada a la salud o a la vida sexual. Asimismo, aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos



²¹ Directiva Administrativa N° 294-MINSA/2020/OGTI, aprobada por R.M. N° 688-2020/MINSA. 5.1 Definiciones Operativas, V Disposiciones Generales, Numeral 5.1.7 Confidencialidad de la Información.

²² Adaptado del Artículo 7 - Principio de consentimiento. Reglamento de la Ley N° 29733 Ley de Protección de Datos Personales.

²³ Definición adaptada a partir del Artículo 18, Ley 29733 Ley de Protección de Datos Personales.

²⁴ Definición adaptada del Artículo 19 y 20, Ley 29733 Ley de Protección de Datos Personales.

²⁵ Numeral 4, Artículo 2 Definiciones, Ley 29733 Ley de Protección de Datos Personales.

personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad.²⁶

- 6.10. Encargado de tratamiento de datos personales:**
 Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento sin la existencia de un banco de datos personales, y por encargo del responsable del tratamiento de datos personales.²⁷
- 6.11. Flujo transfronterizo de datos personales:**
 Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.²⁸
- 6.12. Fuentes accesibles para el público:**
 Bancos de datos personales de administración pública o privada, que pueden ser consultados por cualquier persona, previo abono de la contraprestación correspondiente, de ser el caso.²⁹
- 6.13. Integridad de la Información:**
 Es el atributo de la información de ser correcta y no haber sido modificado, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros. Esta integridad se pierde cuando la información se modifica o cuando parte de ella se elimina.³⁰
- 6.14. Interoperabilidad:**
 La Interoperabilidad es la capacidad de interactuar que tienen las organizaciones diversas y dispares para alcanzar objetivos que hayan acordado conjuntamente, recurriendo a la puesta en común de información y conocimientos, a través de los procesos y el intercambio de datos entre sus respectivos sistemas de información.³¹
- 6.15. Nivel suficiente de protección para los datos personales:**
 Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.³²
- 6.16. Procedimiento de anonimización:**
 Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.³³
- 6.17. Procedimiento de disociación:**
 Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento no es reversible.³⁴



²⁶ Ley 29733 Ley de Protección de Datos Personales Artículo 2. Definiciones, Numeral 5.

²⁷ Ley 29733 Ley de Protección de Datos Personales, Artículo 2. Definiciones, Numeral 7.

²⁸ Ley 29733 Ley de Protección de Datos Personales, Artículo 2. Definiciones, Numeral 10.

²⁹ Ley 29733 Ley de Protección de Datos Personales, Artículo 2. Definiciones, Numeral 11.

³⁰ Directiva Administrativa N° 294-MINSA/2020/DGTI, aprobada por R.M. N° 888-2020/MINSA. 5.1 Definiciones Operativas, V Disposiciones Generales, Numeral 5.1.14 Integridad de la Información.

³¹ Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital Artículo 26.- Interoperabilidad.

³² Ley de Protección de Datos Personales, Artículo 2. Definiciones, Numeral 12.

³³ Ley de Protección de Datos Personales, Artículo 2. Definiciones, Numeral 14.

³⁴ Ley de Protección de Datos Personales, Artículo 2. Definiciones, Numeral 15.



POLÍTICA INSTITUCIONAL DE PROTECCIÓN DE DATOS PERSONALES

P-PDP/001-OSI-GCTIC
90-2022
V1.0

- 6.18. Responsable del tratamiento:**
Es aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales.³⁵
- 6.19. Seguridad de la información:**
Es el conjunto de acciones establecidas con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información.³⁶
- 6.20. Titular de datos personales:**
Persona natural a quien corresponde los datos personales.³⁷
- 6.21. Titular del banco de datos personales:**
Persona natural, persona jurídica de derecho privado o Entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.³⁸
- 6.22. Transferencia de datos personales:**
Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una Entidad pública o a una persona natural distinta del titular de datos personales.³⁹
- 6.23. Transmisión electrónica:**
Es el proceso por el cual se envían los datos de un lugar a otro a través de los medios de las Tecnologías de la Información y Comunicación (TIC), tales como correo electrónico, enlaces, internet, entre otros.⁴⁰
- 6.24. Tratamiento de datos personales:**
Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.⁴¹
- 6.25. Usuario de los activos de información:**
Personas que utilizan o tienen acceso a la información por medios automatizados o manuales. Los usuarios son responsables de conocer y cumplir las políticas, procedimientos y normas establecidas por la entidad.⁴²

7. Declaración de la Política Institucional de Protección de Datos Personales.

- 7.1. El Seguro Social de Salud – ESSALUD, a través del Comité de Gobierno Digital, los responsables del tratamiento y encargados de tratamiento de datos personales en la entidad, respeta la legislación vigente en materia de Protección de Datos Personales, la privacidad de los ciudadanos, el secreto y seguridad de la Información concerniente a las personas, de conformidad con lo previsto en el artículo 2 numeral 6 de la Constitución Política del Perú y lo establecido en la Ley de Protección de Datos**



35 Reglamento de la Ley de Protección de Datos Personales, Artículo 2. Definiciones, Numeral 14

36 Adaptada del Numeral 2.33. 2 Términos y definiciones, ISO/IEC 27000:2014

37 Ley de Protección de Datos Personales, Artículo 2. Definiciones, Numeral 16.

38 Ley de Protección de Datos Personales, Artículo 2. Definiciones, Numeral 17.

39 Ley de Protección de Datos Personales, Artículo 2. Definiciones, Numeral 18.

40 5.1.22 Transmisión electrónica, 5.1 Definiciones Operativas. V Disposiciones Generales, Directiva Administrativa N° 294-MINSA/2020/OGTI, aprobada por R.M. N° 688-2020/MINSA.

41 Ley de Protección de Datos Personales, Artículo 2. Definiciones, Numeral 19.

42 Acapite d), Artículo 117. Principios del Marco de la Arquitectura Digital del Estado Peruano, Decreto Supremo N° 029-2021-PCM



**POLÍTICA INSTITUCIONAL DE PROTECCIÓN
DE DATOS PERSONALES**

P-PDP/001-OSI-GCTIC
90-2022
V1.0

Personales N° 29733 y su Reglamento, aprobado con Decreto Supremo N° 003-2013-JUS.

- 7.2. Los responsables y encargados de tratamiento de datos personales, adoptan las medidas técnicas, legales y organizativas para garantizar la confidencialidad en el tratamiento de los datos personales y evitar su alteración, pérdida, acceso o tratamiento no autorizado; habida cuenta del estado de la tecnología y la naturaleza de los datos y los riesgos a los que están expuestos.
- 7.3. El Seguro Social de Salud – ESSALUD, realiza el tratamiento de datos personales en base a los lineamientos del numeral N° 5 del presente documento.
- 7.4. El Seguro Social de Salud – ESSALUD, establece los recursos y medios administrativos y tecnológicos para que los titulares de datos personales puedan ejercer los derechos de acceso, rectificación, cancelación, oposición y otros derechos contemplados en la Ley.
- 7.5. El titular de los datos personales será el único responsable de los datos que consigne en los formularios con datos falsos, inexactos, incompletos o no actualizados.
- 7.6. El Seguro Social de Salud – ESSALUD, promueve la toma de concientización y capacitación del personal institucional en materia de protección de datos personales y fomenta la mejora continua.
- 7.7. Cualquier cesión a terceros de los datos del titular de datos personales, será comunicada debidamente a los afectados especificando la identidad de los cesionarios y la finalidad con que se van a tratar los datos que se ceden.
- 7.8. La Alta Dirección de ESSALUD, se compromete a brindar los recursos necesarios y disponer la implementación de estrategias y directrices que permitan la adecuada gestión de la seguridad de la información, alineadas a la normativa vigente y en función de la evaluación y tratamiento de los riesgos de seguridad de la información.

