ÍNDICE

1. RESUMEN. 2
2. OBJETIVO. 2
3. ALCANCE. 2
4. ROLES Y RESPONSABLES. 2
4.1 H. Directorio 2
4.2 Delegado de protección de datos 2
4.2.1 Funciones del delegado de protección de datos 3
4.2.2 Independencia y confidencialidad 4
4.2.3 Recursos y formación 4
4.3 Gerencias responsables 4
4.4 Integrantes de Enap 4
4.5 Gerencia de Tecnologías de la Información 5
4.6 Dirección de Seguridad de la Información 5
4.7 Gerencia de Compras y Gestión de Servicios 5
5. DESARROLLO. 5
5.1 Principios generales 5
5.2 Derechos de los titulares 6
5.3 Obligaciones y prohibiciones 6
6. DEFINICIONES 9
7. SANCIONES 11
8. REFERENCIAS 11
9. VIGENCIA. 11

1. RESUMEN.

La presente Política establece los principios, responsabilidades y lineamientos generales que Enap deberá observar en el tratamiento de datos personales, con el objeto de resguardar los derechos de las personas y asegurar que dichos tratamientos se realicen de manera lícita, transparente, proporcional y segura. Para estos efectos, Enap cuenta con un Programa de Protección de Datos Personales basado en la gestión de riesgos, la protección de datos desde el diseño, el respeto de los derechos de los titulares y la mejora continua de sus medidas de control.

2. OBJETIVO.

Esta política tiene por objeto establecer el marco general para la protección y tratamiento responsable de los datos personales que Enap administra en el desarrollo de sus actividades, promoviendo su utilización únicamente para finalidades legítimas y bajo condiciones que establecen las leyes y demás normativa pertinente. Asimismo, busca integrar la protección de datos personales en los procesos, proyectos y relaciones con terceros de Enap, mediante un enfoque preventivo y basado en riesgos, de conformidad con la normativa vigente.

3. ALCANCE.

La presente Política aplica a los/as miembros del Directorio y a las trabajadoras y trabajadores de la Empresa Nacional del Petróleo, Enap Refinerías S.A., Gas de Chile S.A y Enap Sipetrol S.A. y sus filiales actuales o futuras en Ecuador y Egipto, en adelante conjuntamente denominadas “Enap”, “Empresa” o “Grupo de Empresas Enap”, sin perjuicio de la normativa local que resulte aplicable.

La presente Política será aplicable a todas las actividades de tratamiento nacional e internacional de datos personales que Enap realice, tanto en su calidad de Responsable como en su rol de Encargado, de conformidad con las normativas legales vigentes que correspondan en cada caso.

Asimismo, las obligaciones que correspondan serán incorporadas contractualmente en las relaciones con proveedores, prestadores de servicios y demás terceros que traten datos personales por cuenta de Enap, de conformidad con la ley y la normativa interna aplicable.

Las estipulaciones del presente documento deberán interpretarse en concordancia con la naturaleza y el giro de Enap. Además, esta Política se complementa con los demás procedimientos, políticas y normas internas de la Empresa.

4. ROLES Y RESPONSABLES.

4.1 H. Directorio

Corresponderá al H. Directorio aprobar la presente Política y ejercer la supervisión general del Programa de Protección de Datos Personales a través de la Gerencia de Ética y Cumplimiento, así como designar al Delegado de Protección de Datos Personales y procurar que éste cuente con la autonomía, facultades y recursos necesarios para el adecuado ejercicio de sus funciones.

4.2 Delegado de protección de datos

El delegado de protección de datos, en adelante “DPO” tendrá como misión promover una gestión responsable de los datos personales en Enap, asesorando a la Empresa, supervisando el cumplimiento del marco aplicable y contribuyendo a identificar y gestionar oportunamente los

riesgos que puedan afectar los derechos de sus titulares y actuar como enlace con la autoridad competente.

El delegado de protección de datos ejercerá sus funciones con autonomía de criterio en materias de protección de datos personales, mantendrá la confidencialidad respecto de la información a la que acceda con ocasión de sus funciones y podrá desempeñar otras responsabilidades en la medida que éstas no generen conflictos de interés. Enap le proporcionará los medios y recursos razonablemente necesarios para el desempeño de su función.

4.2.1 **Funciones del delegado de protección de datos**

El delegado de protección de datos tendrá a su cargo el cumplimiento de las siguientes funciones:

- Informar y asesorar a los Integrantes de Enap y a los terceros encargados o mandatarios, respecto de las disposiciones legales y reglamentarias relativas al derecho a la protección de los datos personales y a la regulación de su tratamiento, de las instrucciones y normas generales y obligatorias, y de las decisiones emitidas por la Agencia de Protección de Datos Personales.
- Elaborar, revisar, coordinar y supervisar el programa de cumplimiento en materia de protección de datos personales que adopte Enap, junto a las políticas, protocolos, reglas y procedimientos específicos de la Empresa relativos al tratamiento de datos personales.
- Participar y promover la difusión, conocimiento, comprensión y cumplimiento de la presente política y del programa de cumplimiento al interior de la organización, y supervisar que la información se encuentre permanentemente disponible para los integrantes de Enap, para los terceros mandatarios, y para los titulares de datos.
- Supervisar el cumplimiento de la legislación aplicable en materia de protección de datos por parte de la Empresa, lo cual comprende la realización de auditorías, actividades de difusión interna y formación del personal involucrado en el tratamiento de datos.
- Preocuparse de la formación y capacitación permanente en materia de protección de datos personales de todas las personas que, en la organización, participan en las operaciones de tratamiento de datos. Para el cumplimiento de esta función, el delegado podrá recomendar la periodicidad con que deban realizarse tales acciones, y las materias específicas que deben comprender.
- Revisar los controles implementados por la Empresa, identificar posibles incumplimientos y proponer las medidas correctivas que correspondan.
- Apoyar a Enap en la elaboración y actualización del RAT, matrices de riesgo, PIA y otras herramientas similares, con el objetivo de identificar riesgos y realizar su seguimiento, así como proponer controles y estrategias de mitigación frente a los riesgos detectados en cada iniciativa y proyecto que tenga impacto en la protección de datos personales.
- Revisar y emitir opinión sobre las iniciativas y proyectos que contemplen el tratamiento de datos personales.
- Participar en el diseño de nuevos proyectos que impliquen tratamiento de datos personales, promoviendo la implementación de protección desde el diseño y por defecto.
- Actuar como punto de contacto para atender las solicitudes de los Titulares vinculadas al tratamiento de sus datos personales y al ejercicio de sus derechos.
- Actuar como enlace y cooperar con las autoridades de protección de datos.
- Proponer mejoras tecnológicas orientadas a facilitar el tratamiento de datos y minimizar los riesgos operativos relacionados.

- Desarrollar un plan anual de trabajo para el cumplimiento de sus funciones y rendir cuenta de sus resultados, a lo menos, anualmente, ante el H. Directorio. Asimismo, el delegado deberá difundir tanto el plan anual como sus resultados al interior de la organización.
- Absolver las consultas y solicitudes de los titulares de datos dentro del marco de atribuciones que la ley le otorga.

4.2.2 **Independencia y confidencialidad**

El delegado de protección de datos ejercerá sus funciones con autonomía, sin recibir instrucciones respecto de las responsabilidades relacionadas con la protección de datos. Del mismo modo, deberá mantener estricto secreto o confidencialidad respecto de los datos personales a los que acceda en el ejercicio de sus funciones.

4.2.3 **Recursos y formación**

Enap proporcionará al delegado de protección de datos los medios, facultades y recursos materiales indispensables para el ejercicio adecuado de sus funciones. Asimismo, garantizará que el delegado reciba la formación y actualización continua necesaria para mantenerse informado sobre la normativa vigente y las prácticas en materia de protección de datos.

La presente Política será objeto de revisión por parte de la Gerencia de Auditoría Interna, quien la incorporará en su planificación anual de actividades de auditoría. Las pruebas y procedimientos que se diseñen tendrán como finalidad evaluar la observancia de las disposiciones aquí contenidas y detectar áreas susceptibles de mejora.

4.3 Gerencias responsables

Las gerencias que ejecuten o administren procesos o actividades que impliquen tratamiento de datos personales serán responsables, con apoyo del DPO, de incorporar los requisitos establecidos en esta Política y en la normativa interna específica, así como de:

- identificar los tratamientos bajo su responsabilidad y mantener actualizada la información correspondiente;
- determinar las finalidades del tratamiento y verificar, junto al DPO, la existencia de una base de licitud aplicable;
- incorporar oportunamente al DPO en aquellos proyectos, cambios o tratamientos que puedan presentar riesgos relevantes;
- implementar y mantener los controles definidos para los riesgos identificados;
- comunicar oportunamente incidentes, incumplimientos o circunstancias que puedan afectar la protección de los datos personales.

4.4 Integrantes de Enap

Todo/a trabajador/a que, con ocasión de sus funciones, tenga acceso o realice operaciones sobre datos personales deberá:

- tratarlos únicamente para finalidad de la actividad que realiza, asociados al ejercicio de sus funciones y conforme a las instrucciones de Enap;
- acceder únicamente a aquellos datos que resulten necesarios para el desarrollo de sus labores;
- mantener su confidencialidad y adoptar las medidas de seguridad establecidas por Enap;

- abstenerse de comunicar, copiar, utilizar, modificar o eliminar datos personales sin autorización; y
- informar inmediatamente cualquier incidente, pérdida, acceso no autorizado, uso indebido u otra situación que pueda comprometer datos personales.

4.5 Gerencia de Tecnologías de la Información

Responsable de incorporar y mantener, en los sistemas, plataformas e infraestructura tecnológica de Enap, los requerimientos técnicos asociados a la protección de datos personales, implementando los controles de acceso, configuración, trazabilidad, conservación, eliminación y demás medidas que correspondan conforme a las definiciones de las áreas responsables y a la normativa interna. Asimismo, deberá integrar criterios de protección de datos desde el diseño y por defecto en el desarrollo, adquisición, modificación y operación de soluciones tecnológicas que involucren tratamiento de datos personales, coordinándose con el DPO y la Dirección de Seguridad de la Información cuando corresponda.

4.6 Dirección de Seguridad de la Información

Responsable de definir, implementar y supervisar los lineamientos y controles de ciberseguridad destinados a proteger los datos personales frente a accesos, usos, alteraciones, pérdidas, filtraciones o destrucciones no autorizadas. Asimismo, deberá gestionar los riesgos e incidentes de seguridad que puedan comprometer datos personales, coordinar su contención y análisis y proporcionar oportunamente al DPO y a las áreas competentes los antecedentes necesarios para evaluar las medidas y comunicaciones que correspondan.

4.7 Gerencia de Compras y Gestión de Servicios

Responsable de incorporar, en los procesos de contratación de terceros que actúen como Encargados del tratamiento de datos personales por cuenta de Enap, los requisitos contractuales y de idoneidad definidos para estos efectos, actuando conforme a los lineamientos e instrucciones del DPO.

Asimismo, deberá verificar que las áreas usuarias incorporen en su evaluación técnica que los terceros cuenten con condiciones adecuadas para realizar el tratamiento y que los contratos respectivos contemplen las obligaciones de protección de datos personales que correspondan.

5. DESARROLLO.

5.1 Principios generales

Los integrantes de Enap deberán ejercer sus funciones y responsabilidades de acuerdo con los siguientes principios:

5.1.1 **Principio de licitud y lealtad**: Los datos personales sólo pueden tratarse de manera lícita y leal.

5.1.2 **Principio de finalidad:** Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento de los datos personales debe limitarse al cumplimiento de estos fines. No se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el tratamiento sea para fines compatibles con los autorizados originalmente; que exista una relación contractual o precontractual entre el

titular y Enap que justifique el tratamiento de los datos con una finalidad distinta; que el titular otorgue nuevamente su consentimiento; o cuando lo disponga la ley.

5.1.3 **Principio de proporcionalidad:** Los datos personales que se traten deben limitarse estrictamente a aquéllos que resulten necesarios, adecuados y pertinentes en relación con los fines del tratamiento. Los datos personales pueden ser conservados sólo por el período de tiempo que sea necesario para cumplir con los fines del tratamiento, luego de lo cual deben ser suprimidos o anonimizados, sin perjuicio de las excepciones que establezca la ley.

5.1.4 **Principio de calidad:** Los datos personales deben ser exactos, completos, actuales y pertinentes en relación con su proveniencia y los fines del tratamiento.

5.1.5 **Principio de responsabilidad**: Quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios y de las obligaciones y deberes de conformidad a la ley.

5.1.6 **Principio de seguridad:** En el tratamiento de los datos personales, Enap resguardará los daros personales de acuerdo con estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la naturaleza de los datos.

5.1.7 **Principio de transparencia e información:** Los titulares deberán poder acceder de manera clara, precisa y comprensible, a la información necesaria para el ejercicio de los derechos que establece la ley. Para estos efectos, las políticas y las prácticas sobre el tratamiento de los datos personales deberán encontrarse permanentemente accesibles y a disposición de cualquier interesado.

5.1.8 **Principio de confidencialidad:** Quienes tengan acceso a datos personales deberán guardar secreto o confidencialidad acerca de los mismos. Enap establecerá controles y medidas adecuadas para preservar el secreto o confidencialidad. Este deber subsiste aún después de concluida la relación con el Titular.

5.2 Derechos de los titulares

La normativa vigente en materia de protección de datos reconoce al Titular un catálogo de derechos que Enap tiene el deber de garantizar y proteger. Estos derechos, conocidos habitualmente como "ARCOP", constituyen herramientas fundamentales para el ejercicio del control sobre los datos personales y deben ser respetados íntegramente por Enap y su Personal.

Enap respetará y facilitará el ejercicio de los derechos que la normativa reconoce a los titulares de datos personales, incluidos los derechos de acceso, rectificación, supresión, oposición, portabilidad y, cuando corresponda, bloqueo y aquellos asociados a decisiones automatizadas. El ejercicio de estos derechos será gestionado a través de los canales y conforme al procedimiento que Enap establezca para estos efectos, procurando que las solicitudes sean recibidas, analizadas y respondidas dentro de los plazos legales.

Ningún Integrante de Enap deberá rechazar, responder informalmente o resolver por sí solo una solicitud de ejercicio de derechos que deba ser tramitada conforme al procedimiento corporativo.

5.3 Obligaciones y prohibiciones

Sin perjuicio de los procedimientos, normativas y directrices particulares que regulen ciertos tipos de datos, registros o tratamientos específicos, todo integrante de Enap deberá observar

las siguientes obligaciones y deberes al momento de realizar actividades de tratamiento de datos personales:

5.3.1 **Fuentes de licitud**

Todo tratamiento de datos personales efectuado por Enap deberá contar con una base de licitud reconocida por la normativa aplicable.

El área responsable del tratamiento deberá identificar la finalidad y base de licitud aplicable antes de iniciar el tratamiento y mantener evidencia suficiente que permita acreditar dicha determinación.

Cuando un tratamiento se funde en el consentimiento, éste deberá obtenerse y administrarse de acuerdo con los requisitos legales y con la normativa interna aplicable. Cuando se funde en el interés legítimo, deberá evaluarse y documentarse que dicho interés no prevalece indebidamente sobre los derechos y libertades del titular.

5.3.2 **Transparencia de la información**

Enap mantendrá mecanismos adecuados para proporcionar a los titulares información clara, suficiente, oportuna y accesible acerca del tratamiento de sus datos personales.

La información específica exigida por la normativa será proporcionada a través de los avisos de privacidad, formularios, cláusulas contractuales, u otros instrumentos que correspondan según el tratamiento.

La información proporcionada deberá mantenerse actualizada cuando se produzcan cambios relevantes en las finalidades, bases de licitud, destinatarios u otras condiciones del tratamiento.

Cuando Enap obre en calidad de Encargado del tratamiento de datos personales por cuenta de otro Responsable, el tratamiento se regulará mediante un acuerdo de procesamiento de datos (DPA) que cumpla íntegramente con la regulación respectiva.

5.3.3 **Registro del tratamiento de datos (“RAT”) y sus riesgos asociados**

Enap documentará e identificará los datos que trata, las categorías de Titulares, los tipos de bases de datos que gestiona, así como el ámbito territorial en que opera. Dicha información se plasmará en un Registro de Actividades de Tratamiento (RAT).

Del mismo modo, Enap identificará aquellos procesos, actividades corporativas y operaciones, ya sean regulares o ocasionales, que puedan originar o incrementar el riesgo de incurrir en infracciones a la normativa sobre protección de datos personales. Ello se registrará en una herramienta de gestión de riesgos legales (matriz de riesgos).

Tanto el RAT como la matriz de riesgos deberán actualizarse de forma anual, así como cada vez que se produzcan modificaciones en la legislación aplicable. Esta actualización tiene como propósito garantizar una adecuada gestión de los consentimientos y de los derechos de los Titulares.

5.3.4 **Encargados del tratamiento de datos personales**

Cuando Enap encomiende a un tercero el tratamiento de datos personales por su cuenta, la gerencia de Compras y Gestión de Servicios deberá:

- Verificar la existencia de un contrato o instrumento jurídico que regule la relación con el Encargado. Dicho instrumento deberá contemplar expresamente: las finalidades del tratamiento; las instrucciones que debe seguir el Encargado; las medidas de seguridad exigibles; la prohibición de ceder datos a terceros sin autorización previa que cumpla los requisitos legales y contractuales; la prohibición de subcontratar sin consentimiento previo; y la obligación de destruir o devolver los datos personales una vez finalizada la relación contractual.
- Asegurarse de que el área usuaria incorpore dentro de su evaluación técnica la idoneidad del Encargado para realizar el tratamiento conforme a las instrucciones que entregue el DPO.
- El incumplimiento de estas obligaciones se considerará una infracción grave a esta Política, pudiendo dar lugar a la aplicación de las sanciones disciplinarias correspondientes.

5.3.5 **Evaluación del impacto del tratamiento de datos**

Los nuevos tratamientos y las modificaciones relevantes de tratamientos existentes deberán ser evaluados desde una perspectiva de riesgo.

Cuando sea probable que un tratamiento pueda generar un alto riesgo para los derechos de las personas, deberá realizarse una Evaluación del Impacto del Tratamiento de Datos (PIA), con el objetivo de identificar y ponderar los riesgos potenciales relacionados con el cumplimiento normativo, la responsabilidad corporativa y el daño reputacional. La ejecución del PIA será responsabilidad del líder o responsable de la iniciativa, proyecto, producto o servicio correspondiente, contando con asesoría del DPO.

De los resultados del análisis podrá derivarse la necesidad de implementar correcciones, adoptar medidas de reducción de riesgo o, incluso, denegar el tratamiento cuando la actividad proyectada no sea viable en consideración al nivel de riesgo detectado y al umbral de tolerancia establecido por Enap.

La legislación establece casos en los que la realización de un PIA resulta obligatoria:

- Análisis sistemático y exhaustivo de características personales de los Titulares, fundada en tratamiento o decisiones automatizadas, incluyendo elaboración de perfiles, que genere efectos jurídicos de relevancia sobre ellos.
- Tratamiento a gran escala o de carácter masivo de datos.
- Tratamiento que involucre monitoreo u observación sistemática de zonas públicamente accesibles.
- Tratamiento de datos sensibles y especialmente protegidos en los supuestos de excepción al consentimiento que prevé la ley.

5.3.6 **Tratamiento de datos personales sensibles y otras categorías especiales**

El tratamiento de datos personales sensibles se realizará, como regla general, con el consentimiento expreso del titular, salvo en aquellos casos en que la ley autorice su tratamiento sin consentimiento. Cuando se trate de otras categorías de datos sujetas a reglas especiales de protección, Enap deberá observar los requisitos específicos establecidos por la normativa aplicable.

En estos tratamientos, Enap adoptará medidas de protección acordes con la naturaleza de los datos y los riesgos asociados, limitando su tratamiento y acceso a lo estrictamente necesario para el cumplimiento de la finalidad correspondiente.

Cuando estos tratamientos puedan generar un alto riesgo, deberán someterse a los mecanismos de evaluación y control previstos en esta Política y en la normativa interna aplicable.

5.3.7 **Notificación de vulneración**

Ante la ocurrencia de vulneraciones a las medidas de seguridad que causen destrucción, filtración, pérdida o alteración accidental o ilícita de datos personales, cualquier integrante del Personal de Enap deberá notificar de inmediato dicha circunstancia al delegado de protección de datos desde el momento en que tome conocimiento de ella. Esta notificación permitirá que Enap adopte las medidas necesarias para remediar la vulneración y cumplir con el deber de reportarla ante la autoridad competente cuando corresponda.

Enap exigirá idéntica conducta a todo Encargado del tratamiento respecto del cual actúe como Responsable, de manera que éste notifique sin demora cualquier vulneración de seguridad.

6. DEFINICIONES

Para efectos de la presente política se entenderá por:

6.1 Datos personales: Información relacionada con una persona natural identificada o identificable.

6.2 Titular de los datos: La persona natural, identificada o identificable, a la cual se refieren los datos personales. Para efectos de esta política, los titulares de datos son: clientes, potenciales clientes, trabajadores, proveedores o potenciales proveedores y cualquier otro tercero persona natural con el que Enap se relacione.

6.3 Almacenamiento: El proceso de conservación o custodia de información personal en un registro o base de datos.

6.4 Comunicar: El proceso de dar acceso a información personal a otras personas o entidades.

6.5 Consentimiento: Manifestación de voluntad consciente, informada, libre, específica e inequívoca dada por el titular de los datos para que su información personal sea objeto de tratamiento de datos.

6.6 Responsable de datos: La persona o entidad encargada de decidir sobre el tratamiento, medios y fines de los datos personales; y supervisar el cumplimiento de la política de privacidad de datos personales.

6.7 Derechos protegidos por la ley: Abarca los derechos de Acceso, Rectificación, Supresión, Bloqueo, Portabilidad, Oposición y otros establecidos en la ley que pueden ejercer los titulares de datos frente al manejo de sus datos personales por terceros.

6.8 Medidas de seguridad: Acciones tomadas para proteger la información personal de su pérdida, acceso no autorizado, divulgación, alteración o destrucción.

6.9 Vulneración de seguridad: Cualquier incidente que pueda poner en riesgo la privacidad de los datos personales.

6.10 Datos sensibles: Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, que revelen el origen étnico o racial, la afiliación política, sindical o gremial, la situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural.

6.11 Ciclo de Vida del dato: Período durante el cual el dato es tratado por Enap, abarcando desde que este se captura por primera vez hasta que se elimina.

6.12 Dato crítico: Información que puede o no constituir dato personal o dato sensible, y que posee relevancia considerable para la actividad comercial de Enap.

6.13 Encargado del tratamiento de datos o mandatario: Corresponde a la persona natural o jurídica que trata los datos personales por cuenta del Responsable.

6.14 Terceros: Cualquier persona o entidad diferente del Titular, del Responsable, y de los mandatarios o encargados del tratamiento de estos últimos.

6.15 Cesión de datos: Transferencia de datos personales por parte del responsable de datos a otro responsable de datos.

6.16 Evaluación del impacto del tratamiento de datos (PIA): Herramienta de decisión utilizada para identificar y mitigar los riesgos asociados a la protección de datos personales, con el fin de gestionar eficazmente las medidas necesarias para eliminar o mitigar dichos riesgos.

6.17 Tratamiento de datos personales: Cualquier operación u operaciones que permitan de cualquier forma recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales o conjuntos de estos.

7. SANCIONES

El incumplimiento de esta Política y de la normativa interna que la desarrolle podrá dar lugar a las medidas disciplinarias o sanciones que correspondan conforme al Reglamento Interno de Orden, Higiene y Seguridad y demás normativa aplicable, atendida la naturaleza y gravedad del incumplimiento.

Tratándose de proveedores, encargados del tratamiento u otros terceros sujetos a obligaciones contractuales en materia de protección de datos personales, los incumplimientos podrán dar lugar a las consecuencias contractuales que correspondan, sin perjuicio de las acciones legales aplicables.

8. REFERENCIAS

- Ley 19.628 sobre Protección de la Vida Privada y Ley 21.719 que la modifica.

9. VIGENCIA.

Esta Política entrará en vigor el 1 de diciembre de 2026 y deberá ser revisada a lo menos cada dos años.