I. OBJETIVO

Dar a conocer las exigencias de la Ley de Protección de Datos Personales (Ley N° 29733) y su Reglamento a todos los colaboradores de la compañía, así como garantizar su cumplimiento.

II. ALCANCE

Todos aquellos procesos que involucren información de datos personales de los colaboradores, clientes, proveedores de servicios y terceros de Rimac Seguros y Reaseguros / Rimac S.A. Empresa Prestadora de Salud que en adelante llamaremos la Empresa.

III. DEFINICIONES

- **APDP:** Autoridad Nacional de Protección de Datos Personales.
- **Autorización:** Consentimiento previo e informado del titular del dato para llevar a cabo el tratamiento de sus datos personales.
- **Aviso de Privacidad:** Comunicación verbal o escrita generada por el Titular del Banco de Datos Personales, dirigida al titular de los datos personales informando el tratamiento de sus datos personales.
- **Banco de datos personales:** Conjunto organizado de datos personales, automatizado o no, que cuenta con una determinada finalidad, cualquiera que sea la forma de su creación, formación, almacenamiento, organización y acceso; pudiendo inclusive pertenecer los mismos datos personales a más de un banco de datos personales.
- **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.
- **Bloqueo:** Es la medida por la que el encargado del banco de datos personales impide el acceso de terceros a los datos y éstos no pueden ser objeto de tratamiento, durante el periodo de bloqueo.
- **Cancelación:** Es la acción o medida que en la Ley se describe como “supresión”, cuando se refiere a datos personales, que consiste en eliminar o suprimir los datos personales de un banco de datos.
- **Datos personales:** Toda aquella información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables.
- **Datos personales relacionados con la salud:** Es aquella información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo el grado de discapacidad y su información genética.
- **Dato público:** Es el dato que no sea semiprivado, privado o sensible.
- **Datos indispensables:** Son aquellos datos personales de los titulares que son obligatorios para poder iniciar o mantener una relación jurídica con la empresa.
- **Datos opcionales:** Son aquellos datos que La Empresa requiere para ofrecer servicios adicionales.
- **Datos sensibles:** Datos personales referidos al origen racial o étnico de una persona, ingresos económicos, datos relacionados a la salud, opiniones o convicciones políticas, religiosas, filosóficas o morales, afiliación sindical, e información relacionada a la salud o a la vida sexual entre otros.
- **Derechos ARCO:** Derecho de Actualización, Derecho de Rectificación, Derecho de Cancelación y Derecho de Oposición.

- **Días:** Días hábiles.
- **Encargado del tratamiento:** Persona Natural o Jurídica, pública o privada que por sí misma o en asociación con otros, realice el Tratamiento de datos personales en nombre del Responsable del Tratamiento.
- **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.
- **Habeas Data:** Derecho de cualquier persona a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en el banco de datos y en archivos de entidades públicas y privadas.
- **Procedimiento de anonimización:** Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.
- **Procedimiento de disociación:** Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es reversible.
- **Rectificación:** Es aquella acción genérica destinada a afectar o modificar un banco de datos personales ya sea para actualizarlo, incluir información en él o específicamente corregir su contenido con datos exactos.
- **Responsable del Banco de datos personales:** Persona encargada de cada banco de datos personales, y del cumplimiento de las exigencias de la ley sobre el mismo.
- **Responsable del Tratamiento:** Es aquél que decide sobre el tratamiento de datos personales.
- **Titular de datos personales:** Persona natural a quien corresponde los datos personales.
- **Titular del banco de datos personales:** Determina la finalidad y contenido de los bancos de datos personales, el tratamiento de estos y las medidas de seguridad (La Empresa).
- **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.
- **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.

IV. RESPONSABILIDADES

Gobierno de Datos

- Inscribir los bancos de datos personales y mantenerlos actualizados ante la Autoridad nacional competente.
- Inscribir la transferencia de información transfronteriza.
- Mantener actualizada la Política de Protección de Datos Personales de acuerdo a los objetivos estratégicos del negocio, la legislación y la normativa vigente y coordinar su publicación y difusión.
- Definir los encargados de los Bancos / Sub Bancos de Datos que gestiona la compañía.
- Proporcionar la información relativa al tratamiento de datos personales a la Autoridad Nacional de Protección de Datos Personales cuando esta lo requiera, así mismo permitirle el acceso a los bancos de datos personales que la compañía administra.
- Guardar toda la información respecto a la solicitud de los derechos ARCO en medios físicos o digitales.

Seguridad de la Información

- Cumple el rol de Representante de seguridad de los bancos de datos personales, por lo cual será responsable de:
  a) Velar que la Política de Protección de Datos Personales esté alineada de acuerdo a los objetivos estratégicos del negocio, la legislación y la normativa vigente.
  b) Coordinar el cumplimiento e implementación de los controles de seguridad necesarios, en coordinación con las áreas de negocio y tecnología, definidos en la presente política.
  c) Revisar periódicamente la efectividad de los controles de seguridad adoptados para la protección de los bancos de datos personales y generar acciones de mejora.

Áreas de Negocio y Tecnología

- Implementar controles de seguridad definidos en la presente Política en coordinación con las áreas de soporte y gestión de riesgos.

Colaboradores

- Cumplir la presente política y los procedimientos que de esta deriven.
- Notificar cualquier incidente que comprometa la privacidad de la información de nuestros clientes o a cualquier mal uso de la información que puede afectar al cliente o la reputación de la compañía.

Asesor Legal

- Brindar asesoría legal a las distintas áreas de la compañía en cuanto a la absolución de consultas sobre las especificaciones exigidas por la Ley de Protección de Datos Personales y su Reglamento.

Responsable de Banco de datos personales

- Brindar los recursos y dirección en la protección de los datos personales.

Encargado de Banco / Sub Banco de datos personales

- Informar a la Unidad de Gobierno de Datos sobre las modificaciones (captura de nuevos datos personales, eliminación y/o modificación de datos personales ya existentes, procesos de anonimización, entre otros) en los bancos de datos personales a fin que se formalicen los cambios con la Autoridad competente.
- Velar por el cumplimiento de la presente política en materia de protección de datos personales de La Empresa.
- Autorizar la transferencia de información de los datos personales, asignados en los bancos, a terceros.
- Asegurar la formalización contractual respecto de la transferencia de la información de datos personal cuando se realice.
- Responder ante la consulta de un solicitante de los derechos ARCO del banco de datos / sub Banco de datos que le compete.

V. DESARROLLO DE LA POLÍTICA

ORGANIZACIÓN ADMINISTRATIVA

1. La compañía debe definir a los responsables y encargados de cada banco / sub banco de datos personales, los cuales tendrán responsabilidad directa y velarán por el cumplimiento de la presente política.
2. El titular de los Bancos de Datos es La Empresa como persona Jurídica.
3. El representante de los Bancos de Datos es la Vicepresidencia Ejecutiva de Operaciones y Tecnología para Rimac Seguros y Reaseguros, y Gerencia General para RIMAC S.A. Empresa Prestadora de Salud.

GESTIÓN Y TRATAMIENTO DE LOS BANCOS DE DATOS PERSONALES

4. La creación, actualización o supresión de los bancos de datos debe considerar:
   a) La implementación de procedimientos para la creación, actualización, eliminación y transferencia de banco de datos personales.
   b) La creación de banco de datos personales requiere de la implementación previa de los controles de seguridad necesarios para el cumplimiento de la presente política, la Ley No. 29733 y sus normas complementarias.
   c) La creación de bancos de datos, su modificatoria, y/o los mecanismos de captación de datos personales deben ser aprobados previamente por la Gerencia de Gobierno de Datos.

5. La obtención de datos personales y consentimiento del titular de datos personales, debe considerar:
   a) La compañía prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.
   b) Previo a cualquier tratamiento de datos personales, el encargado de cada banco de datos tiene la responsabilidad de garantizar que se cuente con el consentimiento del titular de datos personales.
   c) Previo a la captura de los datos personales, se debe contar con el consentimiento del titular el cual debe ser informado, expreso e inequívoco.
   d) Dicho consentimiento puede ser obtenido de manera verbal en caso se tratara de datos personales, sin embargo, debe ser obtenido por escrito si es que se trata de datos sensibles.
   e) La recopilación de datos personales debe ser necesaria y lícita con relación a las finalidades determinadas. Así mismo, se debe garantizar la calidad de los datos contenidos en el banco de datos personales, y aplicar las medidas de seguridad necesarias que ayuden a prevenir la adulteración, pérdida y desviación de datos personales.
   f) En caso de necesitar efectuar el tratamiento de datos personales de un menor de edad, se requerirá del consentimiento de los padres o tutores de los mismos, según corresponda, salvo excepciones previstas en la Ley y su Reglamento. En caso de personas mayores a 14 años, no será necesario el consentimiento expreso de los padres o tutores en caso se trate de datos aprobados por la Norma.
   g) No será preciso el consentimiento cuando los datos de carácter personal:
      - Se recojan para el ejercicio de las funciones propias de La Empresa en el ámbito de sus competencias, sea contractual, precontractual, laboral, negociación y profesional, cuando los datos figuren en fuentes de acceso público o cuando exista excepciones establecidas por la Ley No. 29733 y sus normas complementarias.
      - Cuando se realicen actividades de disociación o anonimización.
   h) En caso de obtener datos personales sin el previo consentimiento del titular del dato y no exista excepción para su solicitud, se deben implementar medidas para obtener

el consentimiento para tratarlos. Asimismo, se puede tener el primer contacto con el cliente, siempre y cuando la primera acción sea requerir el consentimiento para contactarlo.

6. La transferencia de Datos Personales debe considerar:
   a) Los encargados de cada banco / sub banco de datos deberán asegurarse de que toda transferencia de datos personales cuente con el consentimiento de su titular de datos, salvo excepciones previstas en la Ley y su Reglamento.
   b) Toda transferencia de datos personales, tanto a nivel nacional como internacional, procederá con autorización de cada encargado del banco / sub banco de datos personales, y el medio por el cual se llevará a cabo dicha transferencia de datos deberá cumplir con la política de seguridad de la información vigente. En caso sea necesario efectuar un flujo transfronterizo de datos personales, los responsables de cada banco de datos deben garantizar que el país destinatario mantenga los niveles de protección adecuados conforme a la ley vigente.
   c) En caso de transferencia transfronteriza se debe comunicar a la Gerencia de Gobierno de Datos para su registro.

7. La contratación de terceros que efectúan un tratamiento de datos personales debe considerar:
   a) Todo tercero con quien la compañía comparta información de datos personales deberá considerar y cumplir, como parte del servicio vigente, con las exigencias de la Ley de Protección de datos personales y su reglamento, lo cual deberá ser formalizado mediante un contrato firmado por ambas partes.
   b) Será de responsabilidad de cada área la regularización de los contratos vigentes con terceros mediante la inclusión de las adendas necesarias que contemplen los términos de la ley. De ser el caso, el asesor legal de la compañía, brindará a solicitud el asesoramiento a los responsables de las áreas correspondientes en cuanto a los términos tratados y definidos en el contrato.

EJERCICIO DE DERECHOS DEL TITULAR DE DATOS PERSONALES

8. Se deben almacenar los datos personales de manera que se posibilite el ejercicio de los derechos de su titular.

9. Se debe implementar mecanismos para que el Titular de los datos o los representantes de menores de edad , formulen solicitudes respecto:

   Derecho de Información:

   - Finalidad para la que sus datos serán tratados.
   - Quiénes son o pueden ser sus destinatarios.
   - Identidad y domicilio del titular del banco de datos personales.
   - La transferencia de los datos personales.
   - Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.
   - Tiempo de conservación de los datos.

   Derecho de Acceso:

   - Obtener la información, de manera gratuita, que sobre sí mismo sea objeto de tratamiento en bancos de datos.

- La forma en que sus datos fueron recopilados.
- Razones que motivaron su recopilación.
- A solicitud de quién se realizó la recopilación.
- Transferencias realizadas o que se prevén hacer.

Derecho de rectificación, cancelación y oposición:

- Cuando se hubiere advertido omisión, error o falsedad.
- Cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados. Cuando hubiera vencido el plazo establecido para su tratamiento.
- La empresa se reserva el derecho de mantener la información a fin de dar cumplimiento a normas especiales de prevención de lavado de activos.
- Toda solicitud de rectificación debe ser acompañada de la documentación sustentatoria correspondiente.

10. Los procedimientos de atención, cualquiera que sea el medio (presencial o electrónico), se debe guardar prueba de la consulta y su respuesta. Asimismo, los reclamos realizados, respecto al tratamiento de datos personales debe ser informado a la Unidad de Seguridad de la Información para la coordinación de los planes de acción correctivos.
11. La atención de las solicitudes y reclamos, por parte de los titulares de los datos personales, debe considerar los siguientes plazos:

Solicitud	Tiempo de Atención
Información	08 días contados desde el día siguiente de la presentación de la solicitud.
Acceso	20 días contados desde el día siguiente de la presentación de la solicitud.
Rectificación, Cancelación Oposición	10 días contados desde el día siguiente de la presentación de la solicitud.
Tutela de derechos (APDP)	15 días contados desde la notificación de la solicitud por parte de la APDP (Autoridad de Protección de Datos Personales)

DEBERES DE LOS COLABORADORES

12. Uso inaceptable de la información referida a datos personales.

Las siguientes actividades están prohibidas y se consideran como un uso inaceptable de la información referida a datos personales. La lista es un intento de proporcionar un marco para las actividades que caen en la categoría de uso inaceptable, pero no se limita a:

a) Usar o tratar la información para beneficio propio o de terceros y sin la autorización del titular de la información.

b) Usar la información de datos personales para realizar actividades contrarias a la legislación vigente.
c) Compartir, con otros trabajadores y/o terceros, de manera directa o indirecta la información de datos personales sin la autorización previa de los encargados de los bancos / sub bancos de datos y cumpliendo las políticas establecidas en el presente documento.
d) Ceder directa o indirectamente la información confidencial a terceros sin la autorización debida de parte de La Empresa.
e) Recopilar datos personales mediante la realización de fraudes, engaños y de medios no permitidos por la legislación peruana.

13. Deber de secreto y de confidencialidad.

Todo trabajador y/o tercero que intervenga en cualquier fase del tratamiento de los datos personales está obligado a mantener la confidencialidad y de secreto profesional cuando corresponda de manera indefinida.

SEGURIDAD DE BANCO DE DATOS

14. Gestión de la Seguridad de la Información de Banco de Datos
    a) Los datos personales recopilados por La Empresa debe ser considerada como **INFORMACIÓN CONFIDENCIAL.**
    b) La protección de los datos personales se debe incorporar dentro del Sistema de Gestión de Seguridad de la Información a fin de asegurar el cumplimiento de las medidas de control necesarias en cumplimiento con la normativa vigente.

15. Medidas de Seguridad Técnica en el Uso de Tecnologías de información y comunicación (TIC)
    a) El uso de Tecnologías de la Información como: Bases de Datos, Aplicaciones de negocio, Equipos de Comunicación, Servidores, Sistemas Operativos, entre otros; que soportan la gestión del tratamiento de datos personales, deben implementar los controles de seguridad requeridos en la Ley No. 29733 (Tipo Complejo) y definidos en la Política de Seguridad de la Información de La Empresa.

16. Medidas de Seguridad Física para la protección de datos personales
    a) Para banco de datos con información sensible, el almacenamiento de información en formato físico debe considerar ubicar el banco de datos personales en un ambiente aislado protegido por cerradura o mecanismo similar, donde la responsabilidad del mecanismo de acceso recae en el Área Usuaria.

    b) Para bancos de datos con información no sensible: la información física se debe considerar: Ubicar el banco de datos personales en un gabinete, caja, cajón de un mueble, gaveta, o similar siempre y cuando tenga una cerradura con llave o similar la cual será responsabilidad del área Usuaria.

CAPACITACIÓN Y MONITOREO EN LA PROTECCIÓN DE DATOS PERSONALES

17. Gestión de Incidentes.
    a) La gestión de incidentes que comprometen datos personales debe ser incluido dentro del procedimiento de gestión de incidentes del SGSI de la compañía.

18. Auditoría
    Se debe desarrollar un programa de auditoría respecto de cumplimiento para asegurar la mitigación de los riesgos relacionados a la protección de datos personales. Esta actividad se debe desarrollar como mínimo una vez al año.

19. Capacitación y Compromiso
    a) El programa de creación de conciencia y entrenamiento para la protección de datos personales debe ser incorporado dentro del programa de entrenamiento del SGSI de la compañía.

VI. GENERALES

20. Actualización de la Política.
    a) La Unidad de Seguridad de la Información es responsable de garantizar que la política se mantenga actualizada y sea apropiada a las necesidades de la empresa. La periodicidad para su revisión, actualización o ratificación es de cada 2 años, o cuando ocurran cambios significativos en los procesos internos o en la normativa externa.
    b) Cada actualización del documento deberá ser acompañado de la respectiva notificación y capacitación a los obligados de cumplirla y de conocerla.

21. Excepciones y Sanciones. Se debe considerar:
    a) Cualquier excepción al cumplimiento de la presente política debe ser notificado a la Unidad de Seguridad de la Información para su registro y evaluación.
    b) El incumplimiento del presente documento se considerará como falta grave y será sancionado como tal según el reglamento interno de trabajo.
    c) El incumplimiento del presente documento será sancionado de conformidad con lo previsto en el reglamento interno de trabajo.

VII. DOCUMENTOS RELACIONADOS

CÓDIGO	NOMBRE
POL-091	Política de Seguridad de la Información
Marco Normativo	Ley de Protección de Datos Personales N° 29733
Marco Normativo	Reglamento de la Ley de Protección de Datos Personales N° 29733
Marco Normativo	Directiva de Seguridad de la Información de la Ley de Protección de Datos Personales N° 29733

VIII. RESPONSABLES DEL FLUJO DE APROBACIÓN

Etapa	Área	Cargo	Nombre
Elaboración	Gobierno de Datos	Gestor de Calidad de Datos	Daniel Ayvar
Revisión 1 (contenido)	Seguridad de la Información	Jefe de Seguridad de la Información	José Carlos Vargas
	Seguridad de TI	Jefe de Seguridad TI	Diego Rodríguez
	Legal	Jefe de Asesoría de Contratos	Claudia Montes
	Legal	Gerente de Asesoría y Contratos	Rodolfo Grados
	Gobierno de Datos	Gerente de Gobierno de Datos	Erick Machuca
Revisión (metodología)	Ingeniería de Procesos-Soluciones de Negocio Tecnológicas	Coordinador del Sistema de Control Documentario	Amado Moreno
(riesgo operacional)	Riesgo Operacional	Jefe de Continuidad de negocio	José Garay
(regulación y control)	Auditoría Interna	Auditor General	Roberto León
Aprobación	Administración y Control del Riesgo	Vicepresidente de Administración y Control del Riesgo	Jorge Ortecho
	Comité de Gestión Integral de Riesgos	Comité	Comité Alta Gerencia
Publicación	Ingeniería de Procesos-Soluciones de Negocio Tecnológicas	Coordinador del Sistema de Control Documentario	Amado Moreno

IX. CONTROL DE CAMBIOS

Fecha de creación del documento	22/04/2014 – Versión 01
Reemplazo	**Documento anterior:** **Nombre**: Protección de Datos Personales v1 **Código:** POL-130 **Versión:** 01 **Fecha***:* 22/04/2014