TERMINOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

RIMAC y **EL PROVEEDOR** son responsables de cumplir estrictamente cada una de las obligaciones que se exponen a continuación, sobre la información de **RIMAC** en virtud del presente contrato:

1. Salvaguardas

En todo momento que **EL PROVEEDOR** tenga acceso, almacene o procese información de **RIMAC SEGUROS**, mantendrá controles administrativos, técnicos y físicos destinados a garantizar la privacidad, integridad y confidencialidad de la Información de **RIMAC** ("Salvaguardas") que cumplan con los Estándares Aplicables y las Leyes Aplicables, incluso lo siguiente:

1.1 Acceso Físico

EL PROVEEDOR mantendrá controles de Acceso físico destinados a asegurar las instalaciones, infraestructura, centros de datos, archivos en copia impresa, servidores, sistemas de respaldo y equipamiento relevantes (inclusive dispositivos móviles) usados para Acceder a la Información Protegida, incluso controles para evitar, detectar y responder a ataques, intrusiones u otras fallas del sistema.

1.2 Autenticación de Usuario

EL PROVEEDOR mantendrá una autenticación de usuario, controles de Acceso y asignación de privilegios específicos dentro de los sistemas operativos, aplicaciones, equipamiento y medios.

1.3 Seguridad del Personal

EL PROVEEDOR mantendrá políticas y prácticas de personal que restrinjan el Acceso a la Información de **RIMAC** y tendrá inclusive contratos de confidencialidad por escrito y realizará verificaciones de antecedentes de acuerdo con las Leyes Aplicables sobre todo el personal que Acceda a Información de **RIMAC** o que mantenga, implemente, o administre Su programa de seguridad de la información y las Salvaguardas.

1.4 Registro y Control

EL PROVEEDOR registrará y controlará los detalles de todo Acceso a Información Protegida en las redes, sistemas y dispositivos operados por **EL PROVEEDOR**. Sus sistemas de registro y control deben cumplir con los Estándares Aplicables y **EL PROVEEDOR** deberá mantener todos los registros de Acceso durante al menos 90 días.

1.5 Controles de Malware

EL PROVEEDOR mantendrá controles antimalware actualizados y de marcas líderes del mercado para proteger todas sus redes, sistemas y dispositivos que Acceden a Información Protegida de **RIMAC** contra malware y software no autorizado.

1.6 Parches de Seguridad

EL PROVEEDOR mantendrá controles y procesos destinados a asegurar que sus redes, sistemas y dispositivos (inclusive los sistemas operativos y las aplicaciones) que Acceden a Información Protegida estén actualizados, lo que incluye la implementación inmediata de todos los parches de seguridad cuando estos se emitan, y/o cuando sean requeridos para subsanar fallos de seguridad.

1.7 Gestión de la Cuenta del Usuario

EL PROVEEDOR implementará procedimientos de gestión de la cuenta del usuario para crear, modificar y eliminar de manera segura cuentas de usuario en las redes, los sistemas y los dispositivos a través de los cuales **EL PROVEEDOR** Accede a Información Protegida, lo que incluye el control de cuentas redundantes y el aseguramiento de que los propietarios de la información autoricen debidamente todas las solicitudes de cuenta de usuario.

EL PROVEEDOR es responsable de proteger y cautelar las credenciales de acceso (usuarios y contraseñas, fotocheck y tarjetas de acceso físico) de uso exclusivo del **PROVEEDOR** que le sean asignadas por **RIMAC** para el desempeño de sus funciones, teniendo en cuenta que estas credenciales permiten acceder a los diferentes sistemas informáticos y ambientes físicos de **RIMAC**. **EL PROVEEDOR** entiende y acepta que las credenciales de acceso son de uso personal y por ningún motivo debe revelarlas, transferirlas o compartirlas con terceras personas. **EL PROVEEDOR** reconoce que es responsable de toda acción que se realice con las credenciales de acceso asignadas en los sistemas informáticos de **RIMAC** y las consecuencias que se deriven de un posible mal uso. En caso de que las credenciales asignadas al PROVEEDOR sean comprometidas, EL PROVEEDOR deberá de informar de manera inmediata a RIMAC.

2. **Controles de Acceso**
EL PROVEEDOR mantendrá controles como segregación de funciones, matriz de accesos, registros de logs de acceso y monitoreo de accesos a la información de **RIMAC** para asegurar que solamente las personas que tengan una necesidad legítima de Acceder a la Información Protegida en virtud del Contrato tengan dicho Acceso; finalizará inmediatamente el Acceso a la Información Protegida por parte de una persona cuando ese Acceso ya no sea necesario para el cumplimiento del Contrato; registrará los detalles adecuados de Acceso a la Información Protegida en Sus sistemas y equipamiento, y conservará dichos registros durante al menos 90 días; y será responsable por cualquier Acceso no autorizado a la Información Protegida. En caso el PROVEERDOR cuente con accesos a los sistemas de RIMAC, deberá de informar de forma inmediata a RIMAC cuando los accesos no sean requeridos o el personal que brinda el servicio haya sido desvinculado laboralmente.

3. **Requisitos de Cifrado**
Mediante el uso de un estándar de cifrado vigente no vulnerado en el mercado global, **EL PROVEEDOR** cifrará toda la Información de **RIMAC** que se almacene en dispositivos portátiles o medios electrónicos portátiles; medios lógicos que se mantengan fuera de **RIMAC** o de sus instalaciones, excluyendo los documentos impresos; o transfiera a través de cualquier red que no sea la red interna de la empresa de propiedad o gestionada por **EL PROVEEDOR**.

4. **Capacitación y Supervisión**
EL PROVEEDOR proporcionará capacitación y supervisión continuos (mínimo anualmente) sobre seguridad de la información, privacidad y protección de la información para todo su personal, siempre que acceda a la información de **RIMAC** (incluso, los Terceros Proveedores). Es posible que **RIMAC** le pida proporcionar alguna capacitación adicional que considere razonablemente necesaria para que **EL PROVEEDOR** realice Servicios en virtud del Contrato.

5. **Uso de las Redes, Sistemas o Dispositivos de RIMAC SEGUROS.**
En la medida en que **EL PROVEEDOR** acceda a las redes, los sistemas o los dispositivos propiedad de **RIMAC** o gestionados por **RIMAC** (inclusive los programas de aplicación de interfaz (Application Programming Interface, API), cuentas de correo electrónico corporativas, equipamiento o instalaciones de **RIMAC SEGUROS**) para Acceder a la Información Protegida, deberá cumplir con las instrucciones escritas, los requisitos de sistema y de **RIMAC** disponibles para **EL PROVEEDOR**.

6. **Evaluaciones, Auditorías y Correcciones**

6.1 Evaluación de Seguridad de RIMAC SEGUROS
Si **RIMAC** lo solicita por escrito, **EL PROVEEDOR** asistirá y cooperará de manera razonable durante cualquier evaluación efectuada por **RIMAC** y/o su tercero designado, las ocasiones en que sea requerido, mediante el ofrecimiento de Acceso a personal experto, documentación, infraestructura, oficinas, y lugares y software de aplicación que Accedan a la Información de **RIMAC SEGUROS**. **RIMAC** deberá enviar esta solicitud con un mínimo de quince (15) días calendario de anticipación a la realización de la auditoría. **RIMAC** tratará la información que **EL PROVEEDOR** proporcione en las evaluaciones como su información confidencial.

6.2 Prueba de Vulnerabilidad de RIMAC SEGUROS:
Si **EL PROVEEDOR** accede, almacena o procesa Información o acceda a recursos tecnológicos de **RIMAC** desde sus sistemas o sus sistemas se conectan a la red o a los sistemas internos de **RIMAC SEGUROS**, en ese caso, **RIMAC** podrá llevar a cabo periódicamente pruebas de vulnerabilidad (inclusive prueba de penetración) en los sistemas que **EL PROVEEDOR** utilice para Acceder o almacenar la Información de **RIMAC** en relación con los Servicios. **RIMAC** no realizará pruebas de vulnerabilidad más de dos veces por año, a menos que **EL PROVEEDOR** cambie sustancialmente los Servicios que presta a **RIMAC** en virtud de este Contrato, o con posterioridad a algún Incidente de Seguridad denunciado, de forma que **EL PROVEEDOR** deberá reportar dichos cambios a **RIMAC** dentro de un plazo no menor a dos (2) días luego de la incidencia. Así mismo RIMAC podrá solicitar información al PROVEEDOR de sobre la evaluación de vulnerabilidades y el estado de remediación sobre los recursos tecnológicos que proporcionará a RIMAC.

6.3 Autoevaluación del PROVEEDOR.
EL PROVEEDOR controlará continuamente el riesgo en la Información de **RIMAC** para asegurar que las Salvaguardas se diseñen y mantengan debidamente para impedir el Acceso no autorizado a la Información de **RIMAC** y periódicamente (pero no menos de una vez por año) evaluará y documentará la efectividad de Sus Salvaguardas en Sus redes, sistemas y dispositivos (lo que incluye infraestructura, las aplicaciones y los servicios) usados para Acceder a la Información de **RIMAC**

SEGUROS. **EL PROVEEDOR** deberá proporcionar a **RIMAC** los resultados de la prueba de vulnerabilidad realizada y el estado de las medidas correctivas que se dispongan en las conclusiones a las que se arribe, **RIMAC** tratará estos resultados como su información confidencial.

6.4 Auditorías, Certificaciones e Informes

EL **PROVEEDOR** permitirá que **RIMAC** realice a potestad auditorías de privacidad y de seguridad, realizadas por personal destacado de **RIMAC** o una sociedad auditora externa o una firma nacional o extranjera, que acredite contar con el conocimiento y experiencia requerida

En lugar de una auditoría iniciada por **RIMAC SEGUROS**, a opción de **RIMAC SEGUROS**, **EL PROVEEDOR** pondrá a disposición de **RIMAC** su informe de prueba de penetración más reciente, último informe de auditoría o certificación que deje constancia del cumplimiento por su parte del presente contrato, inclusive su certificación ISO 27001 más reciente, SOC1, SOC2, informes, o Ratificación de Cumplimiento de los Estándares de la Industria de las Tarjetas de Pago (Payment Card Industry, PCI) por los Servicios. **RIMAC** tratará estos resultados como su información confidencial.

6.5 Corrección de Vulnerabilidades y hallazgos de auditoría

Si alguna de las partes identifica que las Salvaguardas del **PROVEEDOR** contienen una vulnerabilidad u hallazgos resultado de las auditorías realizadas por **RIMAC** o una sociedad auditora externa autorizada por el mismo, **EL PROVEEDOR** corregirá o mitigará inmediatamente a su propio costo cualquier vulnerabilidad u hallazgos dentro de un periodo de acuerdo a su criticidad, en un plazo no mayor a treinta (30) días para vulnerabilidades y hallazgos catalogados como críticas, sesenta (60) días para vulnerabilidades y hallazgos catalogados como altas y noventa (90) días para vulnerabilidades y hallazgos catalogados como medias, para lo cual deberá entregar la respectiva evidencia de cierre a **RIMAC SEGUROS**.

Si **RIMAC** identifica las vulnerabilidades, **EL PROVEEDOR** le proporcionará una garantía razonable de que Sus correcciones cumplen con los requisitos del presente contrato. Si **EL PROVEEDOR** no puede corregir o mitigar las vulnerabilidades dentro del periodo de tiempo especificado, deberá notificar inmediatamente a **RIMAC** y proponer recursos razonables. El cumplimiento de esta Sección no reducirá ni suspenderá Sus obligaciones en virtud de la Sección 7 (Respuesta a Incidentes de Seguridad), ni reducirá o suspenderá los derechos de **RIMAC** en virtud de la Sección 14.2 (Suspensión), y 14.3 (Registros; Conservación).

7. Respuesta a Incidentes de Seguridad

7.1 Programa de Respuesta a Incidentes de Seguridad

EL PROVEEDOR mantendrá un programa de Respuesta a Incidentes de Seguridad razonable, basado en las mejores prácticas vigentes del mercado.

7.2 Notificación de Incidentes de Seguridad

Si se entera de algún Incidente de Seguridad, **EL PROVEEDOR** inmediatamente: tomará medidas para minimizar el daño; asegurará la Información de **RIMAC SEGUROS**; notificará a **RIMAC** (en ningún caso más de 24 horas después de descubrir el Incidente de Seguridad) mediante el envío de un correo electrónico a ciberseguridad@**rimac**.com.pe con la información descrita en el siguiente párrafo; y Comunicará a **RIMAC** las medidas y procedimientos llevados a cabo, en virtud de las Leyes Aplicables, a efectos de mitigar los efectos del incidente.

Si se solicitara, **EL PROVEEDOR** proporcionará la información que sea razonable acerca del Incidente de Seguridad, lo que incluye: una descripción de la Información Protegida sujeta al Incidente de Seguridad (lo que incluye las categorías y cantidad de registros de datos y Sujetos de los Datos comprendidos); la fecha y hora del Incidente de Seguridad; una descripción de las probables consecuencias del Incidente de Seguridad; una descripción de las circunstancias que dieron lugar al Incidente de Seguridad (por ej. pérdida, robo, copiado); una descripción de las medidas recomendadas para mitigar cualquier efecto adverso del Incidente de Seguridad; una

descripción de las medidas que **EL PROVEEDOR** propone para abordar el Incidente de Seguridad; y personas de contacto relevantes que estarán razonablemente disponibles hasta que las partes acuerden mutuamente que se resolvió el Incidente de Seguridad. Para los Incidentes de Seguridad que impliquen Información de **RIMAC SEGUROS**, "razonablemente disponible" significa 24 horas por día, 7 días a la semana.

7.3 Medidas Correctivas

EL PROVEEDOR tomará las medidas adecuadas para corregir inmediatamente la raíz de la/las causa(s) de cualquier Incidente de Seguridad, y cooperará en forma razonable con **RIMAC** respecto a la investigación y medidas correctivas que se llevarán a cabo en relación con el incidente. Asimismo, inmediatamente proporcionará a **RIMAC** los

resultados de la investigación y cualquier medida correctiva que se haya implementado.

7.4 Declaraciones No Autorizadas
Excepto en caso de que las Leyes Aplicables lo dispongan de otro modo, **EL PROVEEDOR** no realizará (ni permitirá que ningún tercero realice) ninguna declaración con relación al Incidente de Seguridad que directa o indirectamente haga referencia a **RIMAC SEGUROS**, a menos que **RIMAC** brinde una autorización expresa por escrito.

8. Uso Aceptable de la Información, Equipos y Servicios Informáticos

8.1 En todo momento que el PROVEEDOR accede, procese, almacena información o acceda a recursos tecnológicos de RIMAC, deberá realizar un uso responsable asociado a las actividades del servicio contratado. Así mismo, el PROVEEDOR deberá de informar a RIMAC de cualquier evento que pueda comprometer los recursos informáticos y la información que estos contienen.

8.2 EL PROVEEDOR deberá alinearse y asegurar que el personal que brinda el servicio a RIMAC apliquen estándares de desarrollo seguro en concordancia con los que cuenta RIMAC para el desarrollo de los sistemas y aplicaciones requeridas.

8.3 EL PROVEEDOR debe emplear estándares y buenas prácticas de seguridad de la información para el desarrollo del servicio contratado por RIMAC.

8.4 En caso el PROVEEDOR ingrese a la red de RIMAC empleando sus propios dispositivos, el PROVEEDOR deberá garantizar y evidenciar que cuenta con herramientas de protección a nivel endpoint como antivirus actualizado, parchado de sistema operativo y aplicaciones, permisos de administrador restringidos, DLP, cifrado de disco duro y los que apliquen de acuerdo con lo solicitado por RIMAC.

9. Seguridad para la Adquisición, Desarrollo y Mantenimiento

9.1 EL PROVEEDOR deberá alinearse y asegurar que el personal que brinda el servicio a RIMAC apliquen estándares de desarrollo seguro en concordancia con los que cuenta RIMAC para el desarrollo de los sistemas y aplicaciones requeridas.

9.2 EL PROVEEDOR debe emplear estándares y buenas prácticas de seguridad de la información para el desarrollo del servicio contratado por RIMAC.

9.3 Como parte del ciclo de vida del desarrollo, EL PROVEEDOR debe realizar un análisis seguridad a la aplicación (análisis de vulnerabilidades o Ethical Hacking) a nivel de código y aplicación a ser publicada con la finalidad de identificar vulnerabilidades y estas sean subsanadas en los plazos especificados en la sección 6.5 Corrección de Vulnerabilidades y hallazgos de auditoría.

9.4 EL PROVEEDOR debe garantizar que se informe de forma periódica sobre las actualizaciones o correcciones que se realicen al sistema o aplicación. Además de proporcionar la asesoría y acompañamiento debido.

10. Cumplimiento

10.1 El PROVEEDOR debe de cumplir con los requisitos indicados por RIMAC, así como también con los controles solicitados en las normativas y regulaciones que aplican a RIMAC como la Ley 29733 - Ley de Protección de Datos Personales y su reglamento, Circular G140 SBS, Resolución SBS N° 504-2021 que aprueba el reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.

11. Borrado seguro de la información

11.1 En caso de la desvinculación laboral del personal del PROVEEDOR o al término del servicio que brinda servicios a RIMAC, EL PROVEEDOR deberá de realizar el borrado seguro de la información de RIMAC almacenada, procesada o generada en los equipos empleados para el desarrollo del servicio. Además, EL PROVEEDOR deberá de informar de manera formal a RIMAC la confirmación del borrado de la información.

11.2 Cuando se finalice la relación laboral o ante la solicitud efectuada por RIMAC. El PROVEEDOR cesara el uso de la información confidencial, debiendo devolver a RIMAC toda la información confidencial recibida y destruir toda copia que se haya realizado. Además, deberá de proporcionar una confirmación por escrito en un plazo no mayor a 15 días resuelto el contrato.

12. Subcontratación por parte del proveedor

12.1 En todo momento que el PROVEEDOR realice subcontratación del personal o del

servicio contratado, debe garantizar que el SUMINISTRADOR subcontratado cumpla los puntos expuestos en el presente documento. Además, el SUMINISTRADOR subcontratado debe contar con acuerdos de confidencialidad y protección de datos personales sobre la información de RIMAC.

12.2 Es responsabilidad del PROVEEDOR informar en un plazo no mayor a quince (15) días cualquier modificación con el SUMINISTRADOR subcontratado para el desarrollo del servicio adquirido por RIMAC.

12.3 En caso de que el PROVEEDOR requiera realizar una subcontratación para el desarrollo del servicio, deberá de contar con la autorización de RIMAC.

13. Proceso Jurídico

Si **EL PROVEEDOR** o cualquiera a quien **EL PROVEEDOR** proporcione Acceso a la Información Protegida se ve obligado jurídicamente por un tribunal u otra entidad gubernamental a divulgar Información Protegida, en ese caso, en la medida que lo permita la ley, **EL PROVEEDOR** informará inmediatamente a **RIMAC** acerca de cualquier solicitud y cooperará razonablemente con los esfuerzos de **RIMAC** para impugnar la divulgación, procurar una orden de protección adecuada, o interponer cualquier otra acción legal que **RIMAC** considere adecuada. Excepto en caso de que las Leyes Aplicables lo requieran, **EL PROVEEDOR** no responderá a dicha solicitud, a menos que **RIMAC** lo haya autorizado a hacerlo.

14. Categorías Especiales de Datos

14.1 Cumplimiento de los Estándares de la Industria de las Tarjetas de Pago (Payment Card Industry, PCI).
En la medida que **EL PROVEEDOR** procese información de titulares de tarjetas de crédito, débito, o de otro tipo de pago, sujeta a los Estándares de Seguridad de los Datos de la Industria de las Tarjetas de Pago (Payment Card Industry Data Security Standards, PCI DSS) en relación con Sus Servicios, **EL PROVEEDOR** se asegurará de estar certificado actualmente y de manera demostrable o en cumplimiento de los PCI DSS, según lo documente un tercero auditor independiente calificado para presentar una Declaración de Cumplimiento de los PCI DSS, y mantendrá Su situación de cumplimiento mientras Acceda a dichos datos en relación con el Contrato.

14.2 Suspensión
RIMAC podrá suspender inmediatamente su Acceso a la Información Protegida si **RIMAC** determina razonablemente que **EL PROVEEDOR** no cumple con el presente contrato o la Ley Aplicable.

14.3 Registros y Conservación

14.3.1 Registros
EL PROVEEDOR conservará en su sede habitual registros detallados, exactos y actualizados relacionados con su Acceso a Información de **RIMAC** y suficientes para cumplir con sus obligaciones en virtud del presente contrato. Si se lo solicita, **EL PROVEEDOR** pondrá esos registros a disposición de **RIMAC SEGUROS**. Si **EL PROVEEDOR** Accede a Información de **RIMAC SEGUROS**, dichos registros deberán contener como mínimo:

(a) Su nombre y datos de contacto;
(b) las categorías de destinatarios a quienes se divulgó o divulgará la Información de **RIMAC SEGUROS**;
(c) el nombre y los datos de contacto de su oficial de protección de datos, si lo hubiera;
(d) las categorías de actividades de procesamiento realizadas en nombre de **RIMAC SEGUROS**; y
(e) cuando corresponda, información sobre transferencias internacionales de datos, lo que incluye la identificación de los países a los que se transfiere Información de **RIMAC** y, si correspondiera, la documentación de las salvaguardas convenientes para cubrir las transferencias de Información de **RIMAC SEGUROS**.

14.3.2 Conservación.
EL PROVEEDOR no conservará ni retendrá ninguna Información de **RIMAC** excepto en la medida en que sea necesario para prestar los Servicios en virtud del Contrato. Si **RIMAC** lo solicita, **EL PROVEEDOR** devolverá inmediatamente a **RIMAC** una copia de la Información de **RIMAC SEGUROS**.

(a)

14.3.3 Limpieza de Medios.
EL PROVEEDOR usará un proceso de limpieza de los medios que elimine y

destruya los datos de acuerdo con las directivas en base a los estándares vigentes del mercado.