TÉRMINOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN DE RIMAC SEGUROS Y REASEGUROS

Mediante la suscripción del presente documento, el **PROVEEDOR Y/O TERCERO**, representado por sus apoderados firmantes, quienes declaran que cuentan con facultades suficientes para dar su conformidad a este tipo de documentos, se obliga a cumplir estrictamente la totalidad de las obligaciones relacionadas a los estándares y condiciones de Seguridad de la Información para el tratamiento de la información de RIMAC SEGUROS y que son expuestas a continuación, y en tanto le resulten aplicables tomando en consideración la naturaleza y características del servicio que preste a favor de **RIMAC SEGUROS.**

Para efectos del presente documento, **PROVEEDOR Y/O TERCERO** se entenderá como toda persona natural o jurídica, nacional o extranjera, que mantenga una relación directa o indirecta con la prestación, suministro, comercialización, distribución, instalación, mantenimiento o cualquier actividad vinculada al bien o servicio, al cual, por la propia naturaleza, le sean aplicables los términos, condiciones y medidas de seguridad establecidas. Esta definición incluye, sin limitación y sin importar la naturaleza de su participación, el nivel de vinculación contractual o la modalidad de colaboración, a fabricantes, distribuidores, comercializadores, agentes, subcontratistas, intermediarios, consultores, asesores, representantes, socios estratégicos, aliados comerciales, proveedores, así como brokers, corredores de seguros y cualquier tercero cuya intervención pueda generar obligaciones, responsabilidades o impactos en la seguridad de RIMAC SEGUROS.

1. **Salvaguardas**
   En todo momento que **EL PROVEEDOR Y/O TERCERO** almacene, procese o transfiera 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 las buenas prácticas, estándares y leyes aplicables, incluyendo lo siguiente:

   1.1 Acceso Físico
   EL PROVEEDOR Y/O TERCERO deberá implementar y mantener controles de acceso físico que garanticen la protección de las instalaciones, infraestructura, centros de datos, archivos en copia impresa, servidores, sistemas de respaldo y equipamiento relevantes (inclusive dispositivos móviles) utilizados para acceder a la Información de **RIMAC** ya sea en el desarrollo del servicio contratado o en la interconexión con los sistemas de **RIMAC**. Dichos controles deberán incluir mecanismos para prevenir, detectar y responder ante ataques, intrusiones o cualquier otra falla que comprometa la seguridad del sistema.

   1.2 Autenticación de Usuario
   EL PROVEEDOR Y/O TERCERO mantendrá una autenticación de usuario, considerando el uso de doble factor de autenticación y otros estándares seguros que se encuentren vigentes en el mercado, controles de acceso y asignación de privilegios específicos dentro de los sistemas operativos, aplicaciones, equipamiento y medios.

   1.3 Seguridad del Personal
   EL PROVEEDOR Y/O TERCERO mantendrá políticas y prácticas de personal que restrinjan el Acceso a laInformación de **RIMAC** y tendrá inclusive contratos de confidencialidad por escrito y realizará verificaciones de antecedentes de acuerdo con las Leyes Aplicables sobre todo elpersonal 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 Y/O TERCERO registrará y controlará los detalles de todo Acceso a Información Protegida en las redes, sistemas y dispositivos operados por **EL PROVEEDOR Y/O TERCERO**. Sus sistemas de registro y control deben cumplir con los Estándares Aplicables y **EL PROVEEDOR Y/O TERCERO** deberá mantener todos los registros de Acceso durante al menos 90 días.

   1.5 Controles de software malicioso
   EL PROVEEDOR Y/O TERCERO mantendrá controles actualizados y de marcas líderes del mercado para proteger todas sus redes, sistemas y dispositivos que Acceden a InformaciónProtegida de **RIMAC** contra malware y software no autorizado.

   1.6 Parches de Seguridad
   EL PROVEEDOR Y/O TERCERO mantendrá controles y procesos destinados a asegurar que su infraestructura tecnológica, sistemas y dispositivos (inclusive los sistemas operativos y las aplicaciones) que acceden, almacenan y/o procesan Información de RIMAC 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 Y/O TERCERO implementará procedimientos de gestión 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 Y/O TERCERO** accede a Información de RIMAC,lo que incluye el control de cuentas privilegiadas y el aseguramiento de que los propietarios de la información por parte de RIMAC autoricen debidamente todas las solicitudes de cuenta de usuario.

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

2. Confidencialidad

EL PROVEEDOR Y/O TERCERO debe proteger toda la información confidencial a la que accede en el marco de los servicios que brinda, asegurando que esta información no se divulgue a terceros sin el consentimiento previo de **RIMAC**, excepto cuando la ley lo requiera.

3. Protección de datos personales

EL PROVEEDOR Y/O TERCERO se compromete a cumplir con las normativas de protección de datos vigentes y a implementar las medidas de seguridad necesarias para garantizar la privacidad de los datos personales procesados, evitando su acceso no autorizado, alteración, pérdida o tratamiento indebido.

4. Controles de Acceso

En todo momento que **EL PROVEEDOR Y/O TERCERO** almacene, procese o transfiera información de **RIMAC,** mantendrá controles de seguridad para que solo personal autorizado tenga acceso a datos sensibles mediante métodos de autenticación seguros. Asimismo, **EL PROVEEDOR Y/O TERCERO** debe garantizar que solo el personal que tenga una necesidad legítima de acceder a la información en virtud del contrato tenga dicho acceso. **EL PROVEEDOR Y/O TERCERO** es responsable de notificar inmediatamente si algún colaborador asignado a la prestación del servicio y/o en la interconexión entre sistemas, se ha desvinculado laboralmente de la empresa, a fin de ejecutar los procesos de baja de sistemas correspondientes, garantizando que la información de **RIMAC** sea salvaguardada.

5. Requisitos de Cifrado

En todo momento que **EL PROVEEDOR Y/O TERCERO** almacene, procese o transfiera información de **RIMAC** realizará el uso de un estándar de cifrado vigente no vulnerado en el mercado global.
EL PROVEEDOR Y/O TERCERO considerará cifrar la información en cada estado:

- Datos en reposo, considerar cifrado para el almacenamiento de la información.
- Datos en tránsito, considerar cifrado de transmisión (uso de certificados, redes privadas (VPN) y/o protocolos de comunicación seguros, firewalls y sistemas de detección de intrusos)
- Datos en uso, considerar cifrados en memoria (memoria volátil o servidores seguros)

6. Capacitación y Supervisión

EL PROVEEDOR Y/O TERCERO como parte de sus actividades proporcionará capacitación y supervisión continua (mínimo anualmente) sobre seguridad de la información, privacidad y protección de la información a todo el personal involucrado en la prestación del servicio y/o interconexión de los sistemas, siempre que acceda a la información o recursos de **RIMAC**. La capacitación debe incluir buenas prácticas, manejo de datos sensibles, procedimientos de seguridad y respuesta a incidentes.
Por el lado de concientización **ELPROVEEDOR Y/O TERCERO** debe llevar a cabo programas para fomentar cultura de seguridad de información, esto incluye pruebas de phishing, manejo seguro de contraseñas y prevención de ataques informáticos. **EL PROVEEDOR Y/O TERCERO** deberá llevar a cabo evaluaciones de competencias en tema de Seguridad de Información para verificar que los colaboradores que atienden el servicio apliquen correctamente las prácticas de seguridad impartidas. Estas evaluaciones deben tener un seguimiento y planes de refuerzo para aquellos que no alcancen con el nivel requerido.
Es posible que **RIMAC** solicite al **PROVEEDOR Y/O TERCERO** proporcionar alguna capacitación adicional que considere razonablemente necesaria para que **ELPROVEEDOR Y/O TERCERO** realice el cumplimiento del servicio contratado, así como las evidencias de las capacitaciones y campaña de concientización ejecutadas.

7. Uso de las Redes, Sistemas o Dispositivos de RIMAC SEGUROS.

En la medida en que **EL PROVEEDOR Y/O TERCERO** 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 instalacionesde **RIMAC SEGUROS**) para acceder a la Información, deberá cumplir con las instrucciones descritas a continuación:

EL PROVEEDOR Y/O TERCERO se obliga a que todo su personal encargado de prestar los servicios a favor de **RIMAC SEGUROS**, contará con equipos o dispositivos electrónicos tales como computadoras, laptops, tablets, entre otros, que hayan sido provistos por **EL PROVEEDOR Y/O TERCERO**. En virtud de ello, **EL PROVEEDOR Y/O TERCERO** se compromete a que su personal no use por ningún motivo laptops o equipos personales y/o equipos que no hayan sido otorgados por **EL PROVEEDOR Y/O TERCERO** para el desarrollo de sus funciones, entre ellos, la prestación de los servicios a favor de **RIMAC SEGUROS.**

EL PROVEEDOR Y/O TERCERO se obliga a que dichos equipos cuenten con las especificaciones de seguridad y calidad establecidos por **RIMAC SEGUROS,** los mismos que se encuentran en el Anexo I del presente documento, en caso de que por la naturaleza del servicio que brinda el **PROVEEDOR Y/O TERCERO resulte aplicable**.

EL PROVEEDOR Y/O TERCERO se obliga a mantener a disposición de **RIMAC SEGUROS** y de manera permanente, toda evidencia que sustente que los dispositivos electrónicos cuentan o cumplen con las especificaciones de seguridad exigidos por **RIMAC SEGUROS** conforme lo establecido en el Anexo I. En virtud de lo antes indicado, a sola solicitud de **RIMAC SEGUROS, EL PROVEEDOR Y/O TERCERO** se obliga a enviar la evidencia antes indicada dentro del plazo máximo de tres (03) días hábiles contados desde la fecha en que le sea requerida dicha información, en caso de que por la naturaleza del servicio que brinda el **PROVEEDOR Y/O TERCERO resulte aplicable**.

EL PROVEEDOR Y/O TERCERO declara conocer y aceptar que **RIMAC SEGUROS** se reserva el derecho de realizar auditorías para verificar el cumplimiento de estos lineamientos en cualquier momento del plazo de la prestación de los servicios, ante lo cual notificará la fecha y hora de la auditoría a **EL PROVEEDOR Y/O TERCERO**.

No obstante que dentro de los contratos laborales que suscriba **EL PROVEEDOR Y/O TERCERO** con sus trabajadores establezcan obligaciones de confidencialidad, los trabajadores del **PROVEEDOR Y/O TERCERO** que sean asignados a ejecutar el servicio que brinda **EL PROVEEDOR Y/O TERCERO** a **RIMAC SEGUROS** deberán declarar que se adhieren al Código de Conducta para PROVEEDOR y/o TERCERO es, así como se comprometen a cumplir con las políticas de seguridad de la información establecidas por **RIMAC SEGUROS**.

8. Evaluaciones, Auditorías y Correcciones

8.1 Evaluación de Seguridad de RIMAC

Si **RIMAC** lo solicita, **EL PROVEEDOR Y/O TERCERO** permitirá que se realice de forma coordinada y acordada cualquier evaluación para verificar los controles de seguridad de la información, ya sea efectuada por **RIMAC** y/o un tercero autorizado para este fin; **RIMAC** deberá enviar esta solicitud con un mínimo de quince (15) días calendario de anticipación a la realización de la auditoría y el PROVEEDOR y/o TERCERO deberá responder con un máximo de (15) días calendario posterior al envío de los requerimientos para la evaluación. **RIMAC** tratará la información que **EL PROVEEDOR Y/O TERCERO** proporcione en las evaluaciones como su información confidencial.
Adicionalmente, **RIMAC** podrá realizar visitas in situ, previa coordinación con **EL PROVEEDOR Y/O TERCERO**, con la finalidad de relevar evidencias sobre controles técnicos o de gestión que se hayan implementado para garantizar la seguridad de la información de **RIMAC.**

8.2 Prueba de Vulnerabilidades

Si **EL PROVEEDOR Y/O TERCERO** almacena, procesa, transfiere información o accede a recursos tecnológicos de **RIMAC** desde sus sistemas o sus sistemas se conectan a la red o a lossistemas internos de **RIMAC**, en ese caso, **RIMAC** podrá solicitar al **EL PROVEEDOR Y/O TERCERO** un informe técnico de las pruebas de vulnerabilidades que incluyan las evidencias correspondientes de que los recursos del PROVEEDOR y/o TERCERO no tienen vulnerabilidades o son de bajo impacto. Caso contrario, **RIMAC** podrá solicitar al **EL PROVEEDOR Y/O TERCERO** que se le proporcione las acciones de mitigación o remediación que se han tomado sobre las vulnerabilidades detectadas y relacionadas con los recursos tecnológicos que se utilizan para proporcionar el servicio a **RIMAC**.

8.3 Autoevaluación del PROVEEDOR Y/O TERCERO.

EL PROVEEDOR Y/O TERCERO realizará el monitoreo continuo, a fin de realizar la gestión adecuada del 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 deuna 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**. **EL PROVEEDOR Y/O TERCERO** 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 suinformación confidencial.

8.4 Auditorías, Certificaciones e Informes

EL **PROVEEDOR Y/O TERCERO** permitirá que se realice de forma coordinada y acordadas con **RIMAC** auditorías de privacidad y de seguridad de la información, 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**, a opción de **RIMAC SEGUROS**, **EL PROVEEDOR Y/O TERCERO** 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.

En caso el **PROVEEDOR Y/O TERCERO** no dé las facilidades de lo anteriormente mencionado, se emitirá un informe indicando el incumplimiento de los controles de seguridad de la información y se informará al negocio **RIMAC** los riesgos identificados que afecten a la confidencialidad, integridad y disponibilidad de la información en el alcance del servicio que nos brinda, para que tomen las acciones correspondientes con el PROVEEDOR y/o TERCERO.

8.5 Corrección de Vulnerabilidades y hallazgos de auditoría

Si alguna de las partes identifica que las Salvaguardas del **PROVEEDOR Y/O TERCERO** contienen una vulnerabilidad o hallazgos resultado de las auditorías realizadas por **RIMAC** o una sociedad auditora externa autorizada por el mismo, **EL PROVEEDOR Y/O TERCERO** corregirá o mitigará inmediatamente a su propio costo cualquier vulnerabilidad o 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 larespectiva evidencia de cierre a **RIMAC SEGUROS**.

Si **RIMAC** identifica las vulnerabilidades, **EL PROVEEDOR Y/O TERCERO** le proporcionará una garantía razonable de que sus correcciones cumplen con los requisitos del presente contrato. Si **EL PROVEEDOR Y/O TERCERO** 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 9 (Respuesta a Incidentes de Seguridad), no reducirá o suspenderá los derechos de **RIMAC** en virtud de la Sección
16.2 (Suspensión), y 16.3 (Registros; Conservación).

9. Respuesta a Incidentes de Seguridad

9.1 Programa de Respuesta a Incidentes de Seguridad

EL PROVEEDOR Y/O TERCERO mantendrá un programa de Respuesta a Incidentes de Seguridad razonable, basado en las mejores prácticas vigentes del mercado.
Cualquier incidente que afecte la confidencialidad, integridad o disponibilidad de la información de RIMAC debe ser notificado de inmediato, incluyendo información descrita en el punto 9.2

9.2 Notificación de Incidentes de Seguridad

Si se entera de algún Incidente de Seguridad, **EL PROVEEDOR Y/O TERCERO** 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 descubrirel 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 Y/O TERCERO** 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. acceso no autorizado, incluyendo fuga, modificación, destrucción o eliminación, robo de información e interrupción del servicio.); una descripción de las medidas recomendadas para mitigar cualquier efecto adverso del Incidente de Seguridad; una descripción de las medidas que **EL PROVEEDOR Y/O TERCERO** 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**, "razonablemente disponible" significa 24 horas por día, 7 días a la semana.

9.3 Medidas Correctivas

EL PROVEEDOR Y/O TERCERO 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.

9.4 Declaraciones No Autorizadas

Excepto en caso de que las Leyes Aplicables lo dispongan de otro modo, **EL PROVEEDOR Y/O TERCERO** 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.

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

10.1 En todo momento que **EL PROVEEDOR Y/O TERCERO** almacene, procese, transfiera información o acceda a recursos tecnológicos de **RIMAC**, deberá realizar un uso responsable asociado a las actividades del servicio contratado. Así mismo, **EL PROVEEDOR Y/O TERCERO** deberá de informar a **RIMAC** de cualquier evento que pueda comprometer los recursos informáticos y la información que estos contienen.

10.2 En caso se requiera realizar el intercambio de información como parte del servicio, EL **PROVEEDOR Y/O TERCERO y RIMAC** coordinarán la entrega o intercambio de información mediante el uso canales seguros de comunicación, que de común acuerdo se determine que cumplan con las condiciones de confidencialidad, disponibilidad e integridad de la información para ambas partes. No está permitido el envío de información mediante servicios gratuitos o públicos.

11. Seguridad para la Adquisición, Desarrollo y Mantenimiento

11.1 **EL PROVEEDOR Y/O TERCERO** deberá alinearse y asegurar que los sistemas que desarrolle para RIMAC o que utilice para brindar servicio a **RIMAC**, cumplan con estándares de desarrollo seguro en concordancia con los que cuenta RIMAC para la configuración, desarrollo y mantenimiento de los sistemas y aplicaciones requeridas. (Anexo II).

11.2 Como parte del ciclo de vida del desarrollo, **EL PROVEEDOR Y/O TERCERO** 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 8.5 Corrección de Vulnerabilidades y hallazgos de auditoría.

11.3 **EL PROVEEDOR Y/O TERCERO** 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.

11.4 **El PROVEEDOR Y/O TERCERO** en coordinación con RIMAC debe disponibilizar canales seguros para el intercambio de información que garanticen su integridad y confidencialidad

12. Cumplimiento

12.1 **El PROVEEDOR Y/O TERCERO** 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° 504-202 que aprueba el reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.

13. Borrado seguro de la información

13.1 En caso de desvinculación laboral del personal, finalización del servicio o terminación de la interconexión con los sistemas del **PROVEEDOR y/o TERCERO** que presta servicios a **RIMAC**, este deberá realizar el borrado seguro de toda la información de **RIMAC** que haya sido almacenada, procesada o generada en los equipos utilizados para la prestación del servicio. El borrado deberá efectuarse conforme a las mejores prácticas reconocidas para la eliminación segura de datos. Asimismo, el **PROVEEDOR y/o TERCERO** deberá comunicar formalmente a **RIMAC** la confirmación del borrado realizado.

13.2 Cuando se finalice la relación laboral o ante la solicitud efectuada por **RIMAC**. El **PROVEEDOR Y/O TERCERO** cesará 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.

14. Subcontratación por parte del PROVEEDOR y/o TERCERO

En todo momento que **El PROVEEDOR Y/O TERCERO** realice subcontratación del personal para la atención del servicio o para la interconexión a los sistemas de RIMAC, 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.**

14.1 Es responsabilidad del **PROVEEDOR Y/O TERCERO** informar en un plazo no mayor a quince (15) días, cualquier modificación con el SUMINISTRADOR subcontratado.

14.2 En caso de que el **PROVEEDOR Y/O TERCERO** requiera realizar una subcontratación para el desarrollo del servicio, deberá de contar con la autorización de **RIMAC**.

14.3 En caso de que **El PROVEEDOR Y/O TERCERO** requiera realizar una subcontratación para el desarrollo del servicio, este nuevo actor deberá de alinearse a los lineamientos de seguridad de RIMAC.

15. Proceso Jurídico

Si **EL PROVEEDOR Y/O TERCERO** o cualquiera a quien **EL PROVEEDOR Y/O TERCERO** 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 Y/O TERCERO** 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 Y/O TERCERO** no responderá a dicha solicitud, a menos que **RIMAC** lo hayaautorizado a hacerlo.

16. Categorías Especiales de Datos

16.1 Cumplimiento de los Estándares de la Industria de las Tarjetas de Pago (Payment Card Industry, PCI).
En la medida que **EL PROVEEDOR Y/O TERCERO** almacene, procese o transmita información, en nombre de la entidad, información de tarjetahabientes, o de otro tipo de pago, sujeta a los Estándares de Seguridad de los Datosde la Industria de las Tarjetas de Pago (Payment Card Industry Data Security Standards,PCI DSS) en relación con sus servicios será responsable de la seguridad de dicha información, **EL PROVEEDOR Y/O TERCERO** se asegurará de estar certificado actualmente y de manera demostrable o en cumplimiento con el standard PCI DSS, según lo documente un tercero auditor independiente calificado QSA para presentar una Declaración de Cumplimiento ROC, AOC y mantendrá Su situación de cumplimiento mientras Acceda a dichos datos en relación con el Contrato.

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

16.3 Registros y Conservación

16.3.1 Registros

EL PROVEEDOR Y/O TERCERO 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 Y/O TERCERO** pondrá esos registros a disposición de **RIMAC SEGUROS**. Si **EL PROVEEDOR Y/O TERCERO** 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**.

16.3.2 Conservación.

EL PROVEEDOR Y/O TERCERO 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 Y/O TERCERO** devolverá inmediatamente a **RIMAC** una copia de la Información de **RIMAC SEGUROS**.

16.3.3 Limpieza de Medios.

EL PROVEEDOR Y/O TERCERO 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.

17. Responsabilidad por brechas de Seguridad

En caso una brecha de Seguridad en los sistemas que **EL PROVEEDOR Y/O TERCERO** utiliza para atender el servicio afecte los datos del cliente, **EL PROVEEDOR Y/O TERCERO** será responsable de cubrir los costos de mitigación y cualquier responsabilidad asociada que surja de la misma, en la medida que la ley lo permita.

18. Actualización de las medidas de Seguridad

EL PROVEEDOR Y/O TERCERO debe actualizar y mejorar sus medidas de seguridad conforme evolucione las tecnologías y aparezcan nuevas amenazas, asegurando la protección continua de la información del cliente.

19. Penalidades

El PROVEEDOR Y/O TERCERO reconoce y acepta que el incumplimiento de cualquiera de las obligaciones referidas en estos Términos acarreará la imposición de una penalidad por parte de **RIMAC SEGUROS**, equivalente al 5% de la factura mensual, cuyo importe podrá compensar con la retribución o cualquier otra acreencia pendiente de pago que mantenga **RIMAC SEGUROS** a favor de **EL PROVEEDOR Y/O TERCERO**. De reincidir en un período de 12 meses contados desde la primera penalidad aplicada, se aplicará una penalidad equivalente al 10% de la factura mensual.
Sin perjuicio de la imputación de la penalidad, el incumplimiento de las obligaciones indicadas podrá ser causal de resolución de pleno derecho, bastando para tal efecto, que **RIMAC SEGUROS** remita una comunicación en ese sentido a **EL PROVEEDOR Y/O TERCERO**.

Fecha: _____
Razón o denominación social:
RUC:

Nombre del Representante Legal 1: _____

DNI del Representante Legal 1: _____

Firma: _____

Nombre del Representante Legal 2: _____

DNI del Representante Legal 2: _____

Firma: _____

ANEXO I

Requisito	Especificación mínima	Comentarios	Condición
Sistema Operativo	*Windows 11 - x64 - 24H2* *macOS 15 (Sequoia) o versiones superiores.* *macOS 14 (Sonoma) hasta Ago'2026*	*Seguridad sugiere estas versiones como mínimo para que los hosts reciban parches actualizados.* *Adicionalmente el usuario no debe ser administrador local de su laptop.*	Necesario
Parches de Seguridad	*Parchado up-to-date*	*- Se sugiere que la actualización del sistema operativo sea automática, salvo que la gestión actual del PROVEEDOR y/o TERCERO permita al OS ser parchado en un tiempo prudente.* *- Adicionalmente se sugiere incluir un proceso de parchado o actualización del SW instalado en el sistema operativo.*	Necesario
Antimalware	*Versión estándar pero vigente definida por el PROVEEDOR y/o TERCERO*	*Base de firmas up-to-date*	Necesario
Endpoint DLP	*Versión estándar vigente definida por el PROVEEDOR y/o TERCERO*	*Como mínimo se requieren las siguientes políticas de control de contenido para prevención de fuga de información:* *- PCI-DSS* *- Ley de Protección de Datos Personales (PII)* *- pólizas de seguro* *- HIPAA* *- GDPR*	Necesario
Device Control	*Versión estándar vigente definida por el PROVEEDOR y/o TERCERO*	*Este control debe impedir el copiado de archivos hacía cualquier dispositivo de almacenamiento, principalmente vía USB.* *También se debe impedir el copiado de archivos por trasferencia de archivos empleando protocolos de conexión inalámbrica como Bluetooth*	Necesario

EDR Endpoint Agent	*Versión estándar vigente definida por el PROVEEDOR y/o TERCERO*	*Agente e indicadores de compromiso actualizados up-to-date*	Necesario
Application Control	*Versión estándar vigente definida por el PROVEEDOR y/o TERCERO*	*El PROVEEDOR y/o TERCERO debe llevar el control de SW admitido por su personal*	Deseado
Ofimática Cloud	*Microsoft 365*	*Si Rimac le va proveer herramientas de colaboración, el PROVEEDOR y/o TERCERO debe contar como mínimo con las licencias "Microsoft 365 F1" o "Microsoft 365 F3" y "Microsoft Defender for Office 365 (Plan 1)" del tenant "rimac.com.pe", que permitan usar los siguientes controles:* *- Intune para gestión del equipo* *- MFA* *- Auditoria* *- Anti-phishing* *- Safe Attachments* *- Safe Links* *- Anti-Spam* *- Anti-malware* *- Cloud DLP* *- Colaboración interna (no externa)* *Nota: Si fuera una licencia proporcionada por el PROVEEDOR y/o TERCERO y por ende administrada con su tenant, se deben homologar los controles y a su vez reforzar con un control de CASB.*	Necesario

Agente de Threat Management	*Versión estándar vigente definida por el PROVEEDOR y/o TERCERO*	*Si el PROVEEDOR y/o TERCERO no lo tuviese definido y/o implementado como baseline, nuestro Red Team podría definir un proceso de scanning de esos equipos para identificar posibles desvíos en su configuración.*	Deseado
Endpoint Encryption	*Versión estándar vigente definida por el PROVEEDOR y/o TERCERO*		Necesario
Cliente VPN	*Forticlient VPN - Última versión publicada por Fortinet*		Necesario
Agente NAC	*Aruba - Última versión estándar y estable definida y certificada por Rimac*	*Servicio gestionado por Rimac, sólo se instalaría el agente para tener visibilidad del SW y el acceso a la red de Rimac tanto local.*	Necesario
Browser	*Microsoft Edge (Up-to-date)*	Aplicar políticas definidas por el PROVEEDOR y/o TERCERO para su aseguramiento y la navegación segura. Nota: No se debe instalar Mozilla Firefox	Necesario
	Google Chrome (Up-to-date)	Aplicar políticas definidas por el PROVEEDOR y/o TERCERO para su aseguramiento y la navegación segura. Nota: No se debe instalar Mozilla Firefox	Necesario
URL Filtering	*No aplica*	*El PROVEEDOR y/o TERCERO debe contar con un perfil de navegación que no le permita acceder a servicios públicos como:* *- Streaming* *- Almacenamiento de nube* *- Email personal* *- Redes Sociales* *- Servicios de Transferencia de Archivos* *- Otras categorías propensas a data leakage, ocio o mala reputación.* *Debería acceder sólo a los sites y servicios afines a Rimac y a su vez reforzar con un control DLP el upload de archivos en servicios de uso personal y/o no relacionado a Rimac.*	Necesario

Security Configuration	*Línea Base de Seguridad definida por el PROVEEDOR y/o TERCERO*	*Establecer controles de hardening que controlen como mínimo lo siguiente:* *1. Control y gestión sobre los usuarios locales, el usuario no debe tener acceso a la credencial de administrador local y menos aún ser administrador local.* *2. Habilitar las auditorias locales.* *3. Establecer directivas de configuración seguras de derechos de usuario y opciones de seguridad.* *4. Deshabilitar servicios de windows inseguros e innecesarios (e.g. SMBv1, TFTP, Telnet Client, etc.)*	Necesario

Requisito	**Especificación mínima**	**Comentarios**	**Condición**
Otros (Aplica para VDI)	*Clipboard*	*Para el contexto de trabajo remoto en el cual se use un escritorio virtual por HTTPS o VPN, deshabilitar la funcionalidad de clipboard que impida copiar archivos desde el escritorio virtual de Rimac hacía la PC host.*	Necesario
	Restringir acceso a Command Prompt	*Debe restringirse el uso del cmd.exe y PowerShell.*	Necesario
	No aplica	*Sean On-premises o Cloud, la autorización sólo debe permitir el acceso desde la red interna de Rimac y no desde Internet.*	Necesario
	Restringir acceso de Admin local	*El PROVEEDOR y/o TERCERO no puede ser administrador de la PC.*	Necesario

ANEXO II

Se establecen los siguientes apartados como controles de seguridad en el ciclo de desarrollo:

1. MANEJO Y REGISTRO DE ERRORES

El objetivo principal de la gestión y registro de errores es proporcionar una reacción útil para los usuarios, administradores y equipos de respuesta a incidentes. El objetivo no es crear cantidades masivas de registros, sino crear registros de alta calidad, con información útil y desechando ruido.

Los registros de bitácora de alta calidad a menudo contienen datos confidenciales y también deben ser protegidos según la ley de protección de datos. Esto debe incluir:

- No recoger o registrar información confidencial si no es necesaria.
- Garantizar que toda la información registrada se gestiona de forma segura y es protegida según su clasificación de datos.
- Asegurar que los registros de bitácora no sean almacenados indeterminadamente, sino que posean un ciclo de vida útil.

Si los registros contienen datos privados o confidenciales, éstos se convierten en parte de la información sensible y por lo tanto resulta muy atractiva para los atacantes.

MEJORES PRÁCTICAS	DESCRIPCIÓN
1.1. Mostrar mensajes de error genéricos	Los mensajes de error no deben revelar detalles sobre el estado interno de la aplicación. Por ejemplo, Versiones y nombres de las plataformas empleadas, la ruta del sistema de archivos y la información de la pila no deben exponerse al usuario a través de mensajes de error.
1.2. No divulgue demasiada información en mensajes de error	Los mensajes para errores de autenticación deben ser claros y, al mismo tiempo, estar escritos para que no se divulgue información confidencial sobre el sistema. **Por ejemplo**: los mensajes de error que revelan que el ID de usuario es válido pero que la contraseña correspondiente es incorrecta confirma a un atacante que la cuenta existe en el sistema.
1.3. Sin excepciones no manejadas	Dados los lenguajes y framework utilizados para el desarrollo de aplicaciones web, nunca permita que ocurra una excepción no controlada. Los manejadores de errores deben configurarse para manejar errores inesperados y devolver resultados controlados al usuario.
1.4. Suprimir errores generados por Frameworks	El framework de desarrollo o plataformas pueden generar mensajes de error predeterminados. Estos deben suprimirse o reemplazarse con mensajes de error personalizados, ya que los mensajes generados por el framework pueden revelar información confidencial para el usuario.
1.5. Registrar todas las actividades de autenticación	Cualquier actividad de autenticación, exitosa o no, debe registrarse.
1.6. Registrar todos los cambios de privilegios	Cualquier actividad u ocasión en la que cambie el nivel de privilegio del usuario debe registrarse.
1.7. Registrar actividades administrativas	Cualquier actividad administrativa en la aplicación o cualquiera de sus componentes deben registrarse. Lo mismo aplica a actividades que el negocio pueda definir como críticas.
1.8. Acceso de registro a datos confidenciales	Cualquier acceso a datos confidenciales debe registrarse. Esto es particularmente importante para las corporaciones que tienen que cumplir con los requisitos

MEJORES PRÁCTICAS	DESCRIPCIÓN
	reglamentarios como la Ley de Protección de Datos Personales, PCI u obligaciones contractuales.
1.9. No registre datos inapropiados	Si bien los errores de registro y el acceso de auditoría son importantes, los datos confidenciales nunca deben registrarse de forma no cifrada. Por ejemplo, bajo PCI, sería una violación registrar datos confidenciales en el registro a menos que el registro sea cifrado. Además, puede crear un punto de exposición serio si la aplicación web se ve comprometida.
1.10. Almacenar registros de forma segura	Los registros deben almacenarse y mantenerse adecuadamente para evitar la pérdida de información o la manipulación por parte de intrusos. La retención de registros debe estar alineados a los controles expuestos en la política de registro de auditoría y política de Seguridad en Operaciones proporcionar suficiente información para las actividades forenses y de respuesta a incidentes.

2. PROTECCIÓN DE DATOS

Hay tres elementos clave para la protección de datos: Confidencialidad, Integridad y Disponibilidad. Este estándar asume que la protección de datos se aplica en un sistema de confianza, como un servidor, que ha sido protegido debidamente y dispone de protecciones suficientes.

Las aplicaciones web deben asumir que todos los dispositivos de un usuario puedan ser comprometidos de alguna manera. Cuando una aplicación transmite o almacena información sensible dentro de dispositivos inseguros, como equipos compartidos, teléfonos y tabletas, la aplicación es responsable de que los datos almacenados en estos dispositivos sean cifrados y no pueden ser fácilmente o ilícitamente obtenidos, alterados o divulgados.

Se debe asegurar que la aplicación verificada satisface los siguientes requisitos de protección de datos de alto nivel:

- **Confidencialidad**: los datos deben ser protegidos de observación no autorizada o la divulgación tanto en tránsito como cuando están almacenados.
- **Integridad**: los datos deben protegerse de alteración o eliminación por parte de usuarios no autorizados.

- **Disponibilidad**: los datos deben estar disponibles para usuarios autorizados cuando sea necesario.

MEJORES PRÁCTICAS	DESCRIPCIÓN
2.1. Use HTTPS en todas partes	Idealmente, HTTPS debería usarse para toda su aplicación. Si tiene que limitar dónde se usa, entonces HTTPS debe aplicarse a las páginas de autenticación, así como a todas las páginas después de que el usuario se autentique. Si se puede enviar información confidencial (por ejemplo, información personal) antes de la autenticación, esas características también se deben enviar.
2.2. Deshabilitar el acceso HTTP para todos los recursos protegidos	Para todas las páginas que requieren protección por HTTPS, la misma URL no debe ser accesible a través del canal HTTP inseguro.
2.3. Utilice el encabezado Strict-Transport-Security	El encabezado Strict-Transport-Security garantiza que el navegador no hable con el servidor a través de HTTP.

MEJORES PRÁCTICAS	DESCRIPCIÓN
2.4. Almacenar contraseñas de usuario utilizando un hash con salt, iterativo y fuerte	Las contraseñas de los usuarios deben almacenarse utilizando técnicas de hashing seguras con algoritmos fuertes como PBKDF2, bcrypt o SHA-512. Simplemente cambiar la contraseña una sola vez no protege suficientemente la contraseña. Use hash adaptativo (un factor de trabajo), combinado con un salt.
2.5. Intercambie claves de cifrado de forma segura	Si las claves de cifrado se intercambian o preestablecen en su aplicación, cualquier establecimiento o intercambio de claves debe realizarse a través de un canal seguro.
2.6. Configurar procesos seguros de administración de claves	Cuando las claves se almacenan en su sistema, deben estar debidamente aseguradas y solo accesibles para el personal apropiado según sea necesario. EJEMPLO: AWS Key Management Service (KMS), Azure Key Vault, AWS CloudHSM.
2.7. Configuración débil de TLS en servidores	Los cifrados débiles deben deshabilitarse en todos los servidores. Como mínimo se debe usar TLS 1.2. Por ejemplo, los protocolos SSL v2, SSL v3 y TLS anteriores a 1.2 tienen debilidades conocidas y no se consideran seguras. Además, deshabilite los conjuntos de cifrado NULL, RC4, DES y MD5. Asegúrese de que todas las longitudes de las claves sean superiores a 128 bits, utilice la renegociación segura y desactive la compresión.
2.8. Utilice certificados HTTPS válidos de una CA de buena reputación	Los certificados HTTPS deben estar firmados por una autoridad de certificación acreditada. El nombre en el certificado debe coincidir con el FQDN del sitio web. El certificado en sí debe ser válido y no caducado.
2.9. Deshabilite el almacenamiento en caché de datos utilizando encabezados de control de caché y autocompletar	El almacenamiento en caché de datos del navegador debe deshabilitarse utilizando los encabezados HTTP o metaetiquetas de control de caché dentro de la página HTML. Además, los campos de entrada confidenciales, como el formulario de inicio de sesión, deben tener la configuración autocomplete = Off en el formulario HTML para indicar al navegador que no guarde en caché las credenciales.
2.10. Limite el uso y el almacenamiento de datos confidenciales	Realice una evaluación para garantizar que los datos confidenciales no se transporten o almacenen innecesariamente. Siempre que sea posible, utilice la tokenización para reducir los riesgos de exposición de datos.
2.11. Necesidad del uso de datos confidenciales	Como parte de la evaluación funcional, se debe evaluar con las áreas de negocio la necesidad de extraer y visualizar datos clasificados como Información Confidencial. Aplicabilidad: Analistas funcionales.
2.12. Visualización de datos confidenciales	Como parte de la evaluación funcional, se debe evaluar con las áreas de negocio cuales roles y/o perfiles deben visualizar datos clasificados como Información Confidencial, por ejemplos aquellos relacionados a datos personales, de salud, bancarios, etc. Para aquellos roles y/o perfiles que no se necesite dicha información de manera completa se debe evaluar su no visualización o enmascaramiento. Aplicabilidad: Analistas funcionales, desarrolladores.
2.13. Protección de datos bancarios	Todo nuevo desarrollo o modificación de algún sistema que capture datos bancarios del cliente debe incorporar técnicas de ofuscación y/o enmascaramiento de los campos en los front-end y proteger los registros correspondientes en las bases de datos siguiendo las recomendaciones alineadas a las especificaciones PCI-DSS aplicables (por ejemplo, cifrado

MEJORES PRÁCTICAS	DESCRIPCIÓN
	del número de tarjeta en caso de que por necesidad del negocio sea muy necesario almacenarlo). Aplicabilidad: Analistas funcionales, desarrolladores.

3. CONFIGURACIÓN Y OPERACIONES

MEJORES PRÁCTICAS	DESCRIPCIÓN
3.1. Automatizar la implementación de aplicaciones	La automatización de la implementación de su aplicación, mediante la integración y la implementación continuas, ayuda a garantizar que los cambios se realicen de manera consistente y repetible en todos los entornos.
3.2. Establecer un proceso riguroso de gestión del cambio	Se debe mantener un riguroso proceso de gestión de cambios durante las operaciones de gestión de cambios. Por ejemplo, las nuevas versiones solo deben implementarse después del proceso.
3.3. Definir requisitos de seguridad	Involucre al dueño del negocio para definir los requisitos de seguridad para la aplicación. Esto incluye elementos que van desde las reglas de validación de la lista blanca hasta los requisitos no funcionales, como el rendimiento de la función de inicio de sesión. La definición de estos requisitos por adelantado garantiza que la seguridad esté integrada en el sistema.
3.4. Realizar una revisión de diseño	La integración de la seguridad en la fase de diseño ahorra dinero y tiempo. Realice una revisión de riesgos y modele las amenazas para identificar riesgos clave. Esto ayuda a integrar las contramedidas apropiadas en el diseño y la arquitectura de la aplicación.
3.5. Realizar revisiones de código	Las revisiones de código centradas en la seguridad pueden ser una de las formas más efectivas de encontrar errores de seguridad. Las evaluaciones de código pueden ejecutarse con herramientas automatizadas o manualmente por personal distinto al que realizó la elaboración.
3.6. Realizar pruebas de seguridad	Realice pruebas de seguridad durante y después del desarrollo para garantizar que la aplicación cumpla con los estándares de seguridad y no cuente con brechas de seguridad al pasar a producción. Las pruebas también deben realizarse después de los principales lanzamientos para garantizar que no se introdujeron vulnerabilidades durante el proceso de actualización.
3.7. Endurecer la infraestructura	Todos los componentes de la infraestructura que admiten la aplicación deben configurarse de acuerdo con las mejores prácticas de seguridad y las pautas de protección. En una aplicación web típica, esto puede incluir enrutadores, firewalls, conmutadores de red, sistemas operativos, servidores web, servidores de aplicaciones, bases de datos y marcos de aplicaciones.
3.8. Credenciales en código fuente	Desacoplar del código fuente las configuraciones técnicas necesarias por cada ambiente, estas configuraciones se deben externalizar y ser gestionadas mediante un repositorio de secretos y configuraciones como un Vault o AWS

MEJORES PRÁCTICAS	DESCRIPCIÓN
	Parameter Store.
3.9. Repositorios de código	Es permitido el uso del repositorio GITLAB gestionado por Rimac (https://gitlab.rimac.com/) y el repositorio corporativo de Rimac en GitHub. Está prohibida la publicación de código fuente (Activo de Rimac) en repositorios públicos no corporativos (github externos a Rimac, gitlab, drive, etc.) u otros repositorios no oficiales.
3.10. Definir un plan de manejo de incidentes	Un plan de manejo de incidentes es gestionado y gobernado según el proceso de Respuesta ante Incidentes de Seguridad de Rimac.
3.11. No codifique las credenciales	Las credenciales no deben ser almacenadas directamente dentro del código de la aplicación o texto plano. Se debe garantizar su anonimización.

4. CONTROLES DE SEGURIDAD EN PIPELINES DEVSECOPS

MEJORES PRÁCTICAS	DESCRIPCIÓN
4.1. Controles de Seguridad en pipelines DevSecOps	La construcción de las aplicaciones que serán desplegadas al entorno productivo no debe generar alertas de seguridad. De detectarse alguna el proceso de construcción automatizada debe detenerse. En los ambientes previos es válido que los controles se encuentren en modo monitoreo, es decir, alertando, pero permitiendo la construcción, a fin de que los equipos responsables puedan tomar las acciones correctivas.
4.2. Revisión automatizada de aplicaciones web y API – Herramienta de análisis dinámico	De manera periódica debe revisarse las URL que serán escaneadas con la herramienta adquirida por Rimac hasta alcanzar la cobertura licenciada.
4.3. Detección de secretos en el repositorio	Todo nuevo pipeline debe ejecutar de manera automatizada la detección de secretos usando la herramienta OpenSource Yield.
4.4. Uso de controles de seguridad OpenSource en el Pipeline	Se considera válido la incorporación de herramientas de seguridad OpenSource en el pipeline en los siguientes escenarios: - No se cuenta con una alternativa licenciada por Rimac. - No se cuenta con una cobertura de licencia disponible. Estos casos deben ser sustentados y comunicados al CoE de Seguridad mediante el Advisor de Seguridad en el equipo de DevSecOps.

5. AUTENTICACIÓN

MEJORES PRÁCTICAS	DESCRIPCIÓN
5.1. Desarrolle un fuerte sistema de restablecimiento de contraseña	Los sistemas de restablecimiento de contraseña suelen ser el eslabón más débil de una aplicación. El sistema debe basarse en preguntas difíciles de adivinar y de fuerza bruta. Además, cualquier opción de restablecimiento de contraseña no debe revelar si una cuenta es válida o no, lo que impide la recolección de nombre de usuario.
5.2. Implemente una política de contraseña segura	Las aplicaciones deben reflejar la política de contraseñas de Rimac, considerando el manejo de sesión y reutilización de contraseñas.
5.3. Implementar bloqueo de cuenta contra ataques de fuerza bruta	El bloqueo de la cuenta debe implementarse para evitar ataques de fuerza bruta contra la funcionalidad de autenticación y restablecimiento de contraseña. Después de varios intentos en una cuenta de usuario específica, la cuenta debe bloquearse por un período de tiempo (parametrizable)o hasta que se desbloquee manualmente por parte del administrador del sistema. Además, es mejor continuar con el mismo mensaje de error que indica que las credenciales son incorrectas o que la cuenta está bloqueada para evitar que un atacante obtenga nombres de usuario.
5.4. Almacene las credenciales de la base de datos de forma segura	Las aplicaciones web modernas generalmente consisten en múltiples capas. El nivel de lógica de negocios (procesamiento de información) a menudo se conecta al nivel de datos (base de datos). La conexión a la base de datos, por supuesto, requiere autenticación. Las credenciales de autenticación en el nivel de lógica de negocios deben almacenarse en una ubicación centralizada que esté bloqueada. **La dispersión de credenciales en todo el código fuente no es aceptable**.
5.5. Gestión de claves	Está prohibido mantener información sensible en el código fuente tales como credenciales de base de datos, usuarios de aplicación, credenciales de plataforma AWS (Access Key y Secret Key) y toda información que pueda ser explotada para ejecutar acciones de impacto negativo.
5.6. Las aplicaciones y el middleware deberían ejecutarse con privilegios mínimos	Si una aplicación se ve comprometida, **es importante que la aplicación misma y los servicios de middleware estén configurados para ejecutarse con privilegios mínimos**. Por ejemplo, si bien la capa de aplicación o la capa empresarial necesita la capacidad de leer y escribir datos en la base de datos subyacente, no se deben proporcionar credenciales administrativas que otorguen acceso a otras bases de datos o tablas.

6. GESTIÓN DE SESIONES

MEJORES PRÁCTICAS	DESCRIPCIÓN
6.1. Asegúrese de que los identificadores de sesión sean suficientemente aleatorios	Los tokens de sesión deben generarse mediante funciones aleatorias seguras y deben tener una longitud suficiente para resistir el análisis y la predicción.
6.2. Regenerar tokens de sesión	Los tokens de sesión deben regenerarse cuando el usuario se autentica en la aplicación y cuando cambia el nivel de privilegio del usuario. Además, si el estado de cifrado cambia, el token de sesión siempre debe regenerarse.
6.3. Implementar un tiempo de espera de sesión inactiva	Cuando un usuario no está activo, la aplicación debería desconectarlo automáticamente. Tenga en cuenta que las aplicaciones Ajax pueden realizar llamadas recurrentes a la aplicación restableciendo efectivamente el contador de tiempo de espera automáticamente.
6.4. Implementar un tiempo de espera de sesión absoluto	Los usuarios deben cerrar sesión después de un largo período de tiempo (por ejemplo, de 4 a 8 horas) desde que iniciaron sesión. Esto ayuda a mitigar el riesgo de que un atacante use una sesión secuestrada.
6.5. Destruye sesiones ante cualquier signo de manipulación	A menos que la aplicación requiera múltiples sesiones simultáneas para un solo usuario, implemente funciones para detectar intentos de clonación de sesiones. Si se detecta algún signo de clonación de sesión, la sesión debe destruirse, lo que obliga al usuario real a volver a autenticarse.
6.6. Invalidar la sesión después de cerrar sesión	Cuando el usuario cierra sesión en la aplicación, la sesión y los datos correspondientes en el servidor deben destruirse. Esto asegura que la sesión no pueda revivirse accidentalmente.
6.7. Coloque un botón para cerrar sesión en cada página	El botón de cierre de sesión o el enlace de cierre de sesión deben ser fácilmente accesibles para el usuario en cada página después de que se hayan autenticado.
6.8. Utilice atributos de cookies seguros (es decir, HttpOnly y Secure Flags)	La cookie de sesión debe establecerse con los indicadores HttpOnly y Secure. Esto asegura que la identificación de la sesión no será accesible para los scripts del lado del cliente y solo se transmitirá a través de HTTPS, respectivamente.
6.9. Establecer el dominio y la ruta de la cookie correctamente	El dominio de la cookie y el alcance de la ruta deben establecerse en la configuración más restrictiva para su aplicación. Cualquier cookie con ámbito de dominio comodín debe tener una buena justificación para su existencia.
6.10. Establecer el tiempo de caducidad de la cookie	La cookie de sesión debe tener un tiempo de vencimiento razonable. Deben evitarse las cookies de sesión que no caducan.

7. MÓVIL

MEJORES PRÁCTICAS	DESCRIPCIÓN
7.1. Verificar valores de identificadores	Los valores de identificadores almacenados en el dispositivo y recuperables por otras aplicaciones, como el número de IMEI no se utilicen como tokens de autenticación.
7.2. Protección de datos sensibles	Los datos sensibles no se almacenen sin protección en el dispositivo.

7.3. Borrado de información sensible	Asegurar que la información sensible almacenada en memoria sea sobrescrita tan pronto como no deje de ser requerida, con el fin de mitigar ataques de volcado de memoria.
7.4. Accesibilidad	Verificar que las contraseñas, claves secretas y tokens de APIs se generan dinámicamente en la aplicación móvil.

8. MANEJO DE ENTRADA Y SALIDA

MEJORES PRÁCTICAS	DESCRIPCIÓN
8.1. Realizar codificación de salida contextual	Todas las funciones de salida deben codificar contextualmente los datos antes de enviarlos al usuario. Dependiendo de dónde terminará la salida en la página HTML, la salida debe codificarse de manera diferente. Por ejemplo, los datos colocados en el contexto URL deben codificarse de manera diferente a los datos colocados en el contexto JavaScript dentro de la página HTML.
8.2. Prefiere las listas blancas a las listas negras	Para cada campo de entrada del usuario, debe haber validación en el contenido de entrada. La entrada de la lista blanca es el enfoque preferido. Solo acepte datos que cumplan ciertos criterios. Para las entradas que necesitan más flexibilidad, las listas negras también se pueden aplicar cuando los patrones o caracteres de entrada erróneos conocidos están bloqueados (Por ejemplo, aceptar solo números, solo caracteres, mayúsculas y minúsculas, etc.).
8.3. Usar consultas SQL parametrizadas	Las consultas SQL se deben diseñar con el contenido del usuario pasado a una variable de enlace. Las consultas escritas de esta manera son seguras contra los ataques de inyección SQL. Las consultas SQL no deben crearse dinámicamente utilizando la concatenación de cadenas. Del mismo modo, la cadena de consulta SQL utilizada en una consulta enlazada o parametrizada nunca debe construirse dinámicamente a partir de la entrada del usuario.
8.4. Use tokens para evitar solicitudes falsificadas	Para evitar ataques de falsificación de solicitudes entre sitios, debe incrustar un valor aleatorio que terceros no conocen en el formulario HTML. Este token de protección CSRF debe ser exclusivo para cada solicitud. Esto evita que se envíe una solicitud CSRF falsificada porque el atacante no conoce el valor del token.
8.5. Configure la codificación para su aplicación	Para cada página de su aplicación, configure la codificación utilizando encabezados HTTP o metaetiquetas dentro de HTML. Esto garantiza que la codificación de la página siempre esté definida y que el navegador no tendrá que determinar la codificación por sí solo. Establecer una codificación consistente, como UTF-8, para su aplicación reduce el riesgo general de problemas como Cross-Site Scripting.
8.6. Validar archivos cargados	Al aceptar cargas de archivos del usuario, asegúrese de validar el tamaño del archivo, el tipo de archivo y el contenido del archivo, así como asegurarse de que no sea posible anular la ruta de destino del archivo.

MEJORES PRÁCTICAS	DESCRIPCIÓN
8.7. Use el encabezado Nosniff para el contenido cargado	Cuando aloje contenido subido por el usuario que pueda ser visto por otros usuarios, use el encabezado nosniff X-Content-Type-Options: para que los navegadores no intenten adivinar el tipo de datos. A veces se puede engañar al navegador para que muestre el tipo de datos incorrectamente (por ejemplo, mostrar un archivo GIF como HTML). Siempre deje que el servidor o la aplicación determinen el tipo de datos.
8.8. Validar la fuente de entrada	La fuente de la entrada debe ser validada. Por ejemplo, si se espera una entrada de una solicitud POST, no acepte la variable de entrada de una solicitud GET.
8.9. Utilice el encabezado de opciones de marco X	Use el encabezado X-Frame-Options para evitar que un sitio extranjero cargue contenido en un marco. Esto mitiga los ataques de clickjacking. Para los navegadores más antiguos que no admiten este encabezado, agregue un código Javascript de framebusting para mitigar el Clickjacking (aunque este método no es infalible y puede eludirse).
8.10. Usar encabezados de respuesta HTTP seguros	Los encabezados de Política de seguridad de contenido (CSP), X-XSS-Protection ayudan a defenderse contra los ataques de Cross-Site Scripting (XSS).
8.11. Usar encabezados de respuesta Referrer-Policy	Las cabeceras HTTP de las aplicaciones web deben contener “Referrer-Policy”, la cual ayuda a mantener el protocolo de navegación HTTPS.

9. CONTROL DE ACCESO

MEJORES PRÁCTICAS	DESCRIPCIÓN
9.1. Aplicar comprobaciones de controles de acceso de forma coherente	Siempre aplique el principio de mediación completa, forzando todas las solicitudes a través de un "guardián de puerta" de seguridad común. Esto garantiza que se activen las comprobaciones de control de acceso independientemente de si el usuario está autenticado o no.
9.2. Aplicar el principio de menor privilegio	Utilice un sistema de control de acceso obligatorio. Todas las decisiones de acceso se basarán en el principio del mínimo privilegio. Si no se permite explícitamente, se debe denegar el acceso. Además, después de crear una cuenta, los derechos deben agregarse específicamente a esa cuenta para otorgar acceso a los recursos. El sistema debe de contar y permitir la creación de roles específicos.
9.3. No use referencias directas de objetos para verificaciones de control de acceso	No permita referencias directas a archivos o parámetros que puedan manipularse para otorgar acceso excesivo. Las decisiones de control de acceso deben basarse en la identidad de usuario autenticada y la información del lado del servidor de confianza.
9.4. No utilice reenvíos o redireccionamientos no validados	Un reenvío no validado puede permitir que un atacante acceda a contenido privado sin autenticación. **Los redireccionamientos no validados permiten que un atacante atraiga a las víctimas a visitar sitios maliciosos**. Evite que esto ocurra realizando las comprobaciones de controles de acceso apropiadas antes de enviar al usuario a la ubicación dada.